KAUNO TECHNOLOGIJOS UNIVERSITETAS

FUNDAMENTALIŲJŲ MOKSLŲ FAKULTETAS

TAIKOMOSIOS MATEMATIKOS KATEDRA

Milda Grigaravičienė

PSEUDOATSITIKTINIŲ SKAIČIŲ GENERATORIŲ STATISTINIŲ SAVYBIŲ TYRIMAS

Magistro darbas

Vadovas
doc. dr. E. Sakalauskas

KAUNAS, 2006

KAUNO TECHNOLOGIJOS UNIVERSITETAS

FUNDAMENTALIŲJŲ MOKSLŲ FAKULTETAS

TAIKOMOSIOS MATEMATIKOS KATEDRA

TVIRTINU
Katedros vedėjas
prof. dr. J.Rimas
2005 06 06

PSEUDOATSITIKTINIŲ SKAIČIŲ GENERATORIŲ STATISTINIŲ SAVYBIŲ TYRIMAS

Taikomosios matematikos magistro baigiamasis darbas

Kalbos konsultantas
dr. J. Džežulskienė
2006 05 30

Vadovas
doc. dr. E. Sakalauskas
2006 06 03

Recenzentas
doc.dr. R. Plėštys
2006 06 01

Atliko
FMMM-4 gr. stud.
M. Grigaravičienė
2006 05 25

KAUNAS, 2006

KVALIFIKCINĖ KOMISIJA

Pirmininkas: Leonas Saulis, profesorius (VGTU)

Sekretorius: Eimutis Valakevičius, docentas (KTU)

Nariai: Algimantas Jonas Aksomaitis, profesorius (KTU)

Vytautas Janilionis, docentas (KTU)

Vidmantas Povilas Pekarskas, profesorius (KTU)

Rimantas Rudzkis, profesorius (MII)

Zenonas Navickas, profesorius (KTU)

Arūnas Barauskas, UAB „Elsis“ generalinio direktoriaus pavaduotojas

Grigaravičienė M. Analysis of pseudorandom number generator‘s statistical features : Master‘s work in applied mathematics / supervisor dr. assoc. prof. E. Sakalauskas; Department of Applied mathematics, Faculty of Fundamental Sciences, Kaunas University of Technology. – Kaunas, 2006. – 46 p.

SUMMARY

Pseudorandom number generator‘s statistical features were analyzed in this work. Pseudorandom numbers are applied in many fields, that‘s why it‘s important for them to satisfy following requirements:

- to have uniform distribution,
- to be uncorrelated.

Hypothesis that random numbers are distributed uniformly is checked by Pearson χ^2 test. Hypothesis that autocorrelation function is equal to zero is checked by Box Ljung test.

During investigation it was noticed, that in all ways generated random numbers didn’t have uniform distribution, except linear congriuential generator. Applying different transformations was set, that for combinations v1-v8 when using parabola, transformed random numbers had uniform distribution. Arcsine was the best transformation for nonlinear congriuential generator. While testing hypothesis about autocorrelation function’s equality to zero was noticed, that zero hypothesis rejection or not depends on:

- random numbers generation algorithm,
- generated sample size,

The best generator, which satisfied requirements, is linear congriuential generator, but it is not suitable, because it is too predictable. Nonlinear congruential generator is chosen as the best one, because its statistical features are closest to the linear generator.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Atsitiktiniai skaičiai (AS) gali turėti daug taikymų. Pavyzdžiui [5]:

1. Sprendimų priėmimas. Žinomi atvejai, kai sprendimai priimami metant monetą ar lošimo kauliuką. Sklinda gandai, kad kai kurie dėstytojai tokiu būdu rašo įvertinimus. Kartais svarbu priimti visiškai nešališką sprendimą. Atsitiktinumas taip pat yra esminė lošimų teorijos optimalios strategijos dalis.
2. Pramogos. Lošimo kauliukų ridenimas, kortų kaladės maišymas, ruletės rato sukimas yra kiekvienam patrauklūs laiko praleidimo būdai. Šie paprasti AS panaudojimai davė pradžią pavadinimui „Monte Karlo metodas“ – terminui, apibūdinančiam bet kokį AS naudojantį algoritmą.
3. Kriptografija. AS naudojami informacijos šifravimui, raktų generavimui.
4. Atranka. Dažnai yra nenaudinga tirti visus atvejus, todėl atsitiktinė imtis parodo, koks būtų „tipinis“ elgesys.
5. Programavimas. AS naudojami algoritmų tikrinimui.

Šio darbo tikslas – ištirti 9 pasiūlytus kriptografijai tinkamus generatorius, palyginti jų savybes su tiesinio kongriuentinio generatoriaus savybėmis. Lyginimas atliekamas su šiuo generatoriumi, nes yra žinoma, kad jo savybės yra tinkamos t.y. juo generuoti AS yra nekoreliuoti, o AS pasiskirstymas yra tolygus. Pastarasis reikalavimas yra labai svarbus kriptografijoje. Tiesinis kongriuentinis generatorius kriptografijai neturėtų būti taikomas, nes yra per daug nuspėjamas.

Darbo uždaviniai:

- Apibrėžti statistines savybes, kurios charakterizuotų generatoriaus kokybę. Tam pasirenkamos autokoreliacijos funkcija ir histograma.
- Atlikti įvairių AS generatorių statistinių savybių tyrimą. Skaičiuojamos histogramos stulpelių reikšmės, proceso autokoreliacijos funkcija, spektras ir spektrinis tankis.
- Mažiausių kvadratų metodu rasti funkcijas transformuojančias AS skirstinį į tolygųjį.
- Parinkti testus hipotezių apie autokoreliacijos funkcijos lygybę nuliui, bei AS pasiskirstymo pagal tolygųjį skirstinį tikrinimui.
- Sukurti grafinę vartotojo sąsają, kurioje būtų realizuota: AS generavimas, transformavimas, grafikų braižymas ir hipotezių tikrinimas.

Gauti rezultatai buvo pristatyti konferencijoje „Matematika ir matematikos dėstymas – 2006” bei VI-oje studentų konferencijoje „Taikomoji matematika“ (2006 m.).

1. BENDROJI DALIS

1.1 ATSITIKTINIŲ SKAIČIŲ GENERATORIŲ APŽVALGA

Yra dvi didelės atsitiktinių skaičių generatorių šeimos: tiesiniai ir netiesiniai generatoriai [15]. Kriptografai nesinaudoja tiesiniais algoritmais, nes jie yra nuspėjami. Tiesiniai atsitiktinių skaičių generatoriai yra dažniausiai naudojami Monte Karlo modeliavime. Jų generuojami skaičiai nėra atsitiktiniai. Generatoriai naudoja deterministinius algoritmus, todėl teisingiau juos būtų vadinti pseudoatsitiktinių skaičių generatoriais. Jų sukuriamos skaičių sekos yra tik panašios į tikras atsitiktines sekas. Toliau šiame darbe pseudoatsitiktiniai skaičiai bus vadinami tiesiog atsitiktiniais skaičiais (AS).

Atsitiktiniams skaičiams gauti naudojami šie metodai:

1) mechaniniai (kauliuko, monetos metimas, lošimo ruletė, raštelio “iš kepurės“ traukimas, ir pan.);
2) fizikiniai (įelektrintų dalelių srautų, neutronų srautų, šiluminių procesų ir pan. panaudojimas);
3) atsitiktinių skaičių lentelės;
4) pseudoatsitiktiniai generatoriai.

Labiausiai yra paplitę rekurentiniai atsitiktinių skaičių generatoriai, realizuojami kompiuteriais. Pradinio skaičiaus pasirinkimas pilnai apsprendžia tokią seką (t.y., seka yra determinuota), tačiau daugelis jos savybių yra analogiškos atsitiktinai išrinktų reikšmių sekos savybėms, kas ir lemia modeliavimo sėkmę [14].

AS generatoriai dažniausiai susideda iš [16]:

- pagrindinio generatoriaus, apibrėžiamo vėliau,
- kai kurių generatorių turimos atsitiktinių skaičių maišymo dalies,
- transformacijos į norimą tikimybinį skirstinį.

Štai keturios dažniausiai pasitaikančios pagrindinių generatorių rūšys:

- tiesinis kongriuentinis (TKG)
- sudėties su perpildymu ir atimties su skolinimu (angl. *Add-with-carry and subtract-with-borrow* (AWCG, SWBG))
- daugybos su perpildymu (angl. *Multiply-with-carry* (MWCG))
- atvirkštinis kongriuentinis (AKG).

Tiesinis kongriuentinis generatorius

Tiesinis kongriuentinis generatorius (TKG) yra vienas iš seniausių ir geriausiai žinomų AS generavimo algoritmų. Teorija, kuria jis grindžiamas yra suprantama, jis lengvai realizuojamas ir

greitas. Kaip bebūtų, yra žinoma, kad šios generatorių klasės savybės nėra idealios. TKG apibrėžiami rekurentiniu ryšiu:

$$X_{n+1} = aX_n + c(mod\, m). \quad \textbf{(1.1.1)}$$

Kita atsitiktinė reikšmė X_{n+1} apskaičiuojama naudojantis prieš tai buvusia reikšme X_n, skaitinėmis konstantomis a ir c, ir skaitiniu moduliu m. Reikšmė $aX_n + c$ apskaičiuojama moduliu m ir taip gaunamas naujas atsitiktinis skaičius X_{n+1}.

TKG didžiausias periodas yra *m*, tačiau dažnai yra mažesnis. Kitos trys sąlygos yra būtinos ir pakankamos, tam kad būtų pasiektas pilnas periodo ilgis *m*:

1. *c* ir *m* turi būti tarpusavyje pirminiai,
2. kiekvienam pirminiam *p*, tokiam, kad *p* dalina *m*, *a-1* yra *p* kartotinis
3. *a-1* yra 4 kartotinis.

Nei vienas iš TKG neturėtų būti naudojamas ten, kur yra svarbus kokybiškas atsitiktinumas. Pavyzdžiui, jis nėra tinkamas Monte Karlo modeliavimui, nes atsiranda autokoreliacija.

Nustačius X_n, skaičiuojamas atitinkamas realus skaičius:

$$R_n = \frac{X_n}{float(m)} \text{ arba } R_n = \frac{X_n}{float(m-1)}.$$

Kai dalinama iš m, R_n reikšmės yra pasiskirsčiusios intervale $[0,1)$. Jei norima, kad R_n būtų pasiskirsčiusios intervale $[0,1]$, reikėtų dalinti iš $(m-1)$. Reikalingas tolygumas, kai tikimybė pasirodyti reikšmei R_n yra lygi tikimybei, kad pasirodys bet kokia kita reikšmė R_n, o R_n vidurkis yra artimas 0.5 [18,19,22].

Sudėties su perpildymu ir atimties su skolinimu generatoriai

Sudėties su perpildymu generatoriai (AWCG) yra tokio pavidalo:

$$x(n) = x(n-s) + x(n-r) + carry\, mod\, \mathbf{M}. \quad \textbf{(1.1.2)}$$

Atimties su skolinimu generatoriai (SWBG) yra tokio pavidalo:

$$x(n) = x(n-s) + x(n-r) - carry\, mod\, \mathbf{M}. \quad \textbf{(1.1.3)}$$

Šie generatoriai yra žymiai ilgesnio periodo (nuo 10^{200} iki 10^{500}) nei TKG ir yra beveik tokie pat greiti kaip ir TKG [16].

Daugybos su perpildymu generatoriai

Daugybos su perpildymu generatoriai (MWCG) yra tokio pavidalo:

$$x(n) = a \cdot x(n-1) + carry\, mod\, \mathbf{M}. \quad \textbf{(1.1.4)}$$

Su daugikliu *a*, kuris pasirenkamas iš didelio rinkinio lengvai randamų sveikų skaičių, periodas yra $a \cdot 2^{31} - 1$. Kai $a = 2^{30}$ eilės, periodas siekia 2^{60} [16].

Netiesinis kongriuentinis generatorius

Netiesinis kongriuentinis generatorius (NKG) yra tokio pavidalo:

$$x_{n+1} = f(x_n) \bmod M , \qquad \textbf{(1.1.5)}$$

kur $f(\cdot)$ yra tam tikra netiesinė funkcija [20].

Atvirkštinis kongriuentinis generatorius

Šio generatoriaus (AKG) yra du variantai: pasikartojantis AKG

$$x_n = a\bar{x}_{n-1} + b(mod\, m); \qquad \textbf{(1.1.6)}$$

ir tikslus AKG

$$x_n = \overline{an + b}(mod\, m); \qquad \textbf{(1.1.7)}$$

Abiejose lygybėse $\bar{c}$ žymi dauginamąją „inversiją“ moduliu *m*, tokią, kad $c\bar{c} \equiv 1(mod\, m)$ kai $c \neq 0$, ir $\bar{0} = 0$. AKG sudarymui reikia pasirinkti modulį *m*, daugiklį *a*, pridedamą narį *b*, ir pradinę reikšmę x_0 [22].

Sudėtinis pasikartojantis generatorius

Vis dažniau pradedamos naudoti ilgos AS sekos. Tokiu būdu tampa reikalingi patikimesni ir su ilgais periodais generatoriai. Vienas iš variantų yra sudėtinių pasikartojančių generatorių klasė (SPG) pagrįsta aukštesnės eilės pasikartojimu [15]:

$$x_n = (a_1 x_{n-1} + ... + a_k x_{n-k})mod\, m . \qquad \textbf{(1.1.8)}$$

Duotam pirminiam moduliui *m*, toks generatorius gali turėti periodą $m^k - 1$. Kai kurie gali turėti žymiai geresnes struktūrines savybes, nei paprastas TKG su tokiu pačiu moduliu, ir būti toks pat greitas ir lengvai realizuojamas.

Fibonačio generatoriai

Pirmasis Fibonačio generatorius

$$N_{i+1} = (N_i + N_{i-1})mod\, M \qquad \textbf{(1.1.9)}$$

nėra geras AS generatorius [20].

Vėlinantis Fibonačio generatorius

Vėlinantis Fibonačio generatorius yra AS generatoriaus pavyzdys. Ši AS generatorių klasė yra tiesinių kongriuentinių generatorių patobulinimas. Jie pagrįsti Fibonačio sekos apibendrinimu [21].

Fibonačio seka gali būti apibrėžiama rekurentiniu sąryšiu:

$$S_n = S_{n-1} + S_{n-2}\ . \qquad \textbf{(1.1.10)}$$

Naujas narys yra paskutinių dviejų sekos narių suma. Galima užrašyti taip:

$$S_n = S_{n-j}(*)S_{n-k}(mod\ M),\ 0 < j < k\ . \qquad \textbf{(1.1.11)}$$

Šiuo atveju, naujas narys yra tam tikra bet kurių, prieš tai buvusių narių kombinacija. *M* yra 2 laipsnis, dažniausiai 2^{32} arba 2^{64}. Operatorius $(*)$ žymi bendrą dvejetainį veiksmą. Tai gali būti sudėtis, atimtis, daugyba, arba pobitinė XOR operacija. Šio tipo generatorių teorija yra sudėtinga ir gali būti nelengva pasirinkti atsitiktines reikšmes *j* ir *k*. Šio tipo generatoriai naudoja paskutines *k* reikšmių. Jei naudojama sudėties operacija, generatorius vadinamas sudėtiniu vėlinančiu Fibonačio generatoriumi (SVFG). Jei naudojama daugyba – dauginamuoju vėlinančiu Fibonačio generatoriumi (DVFG). Jei naudojama XOR operacija, vadinamas bendriniu grįžtamo ryšio postūmio registru (angl. *Generalised Feedback Shift Register*). Merseno Tvisterio (angl. *Mersene Twister*) algoritmas yra atskiras GFSR atvejis.

Sudėtinis vėlinantis Fibonačio generatorius yra:

$$x_n = x_{n-j} + x_{n-k}\left(mod\ 2^m\right),\ j < k\ . \qquad \textbf{(1.1.12)}$$

Pastaraisiais metais, SVFG tapo populiarus, nes yra lengvai realizuojamas, skaičiavimai greiti ir lengvai praeina statistinius testus, ypač, kai vėlinimas *k* yra pakankamai didelis (pvz. $k = 1279$). Maksimalus periodas yra $\left(2^k - 1\right)2^{m-1}$ ir turi $2^{(k-1)\times(m-1)}$ skirtingų, pilno periodo ciklų. Kitas SVFG privalumas yra tai, kad šiuos generatorius galima realizuoti tiesiogiai dirbančius su slankaus kablelio skaičiais, išvengiant sveikų skaičių vertimo į slankaus kablelio skaičius, kas būna naudojant kitus generatorius. Skirtingos sekos kuriamos kiekvienai sekai priskiriant skirtingus ciklus.

Dauginamasis vėlinantis Fibonačio generatorius yra:

$$x_n = x_{n-j} \times x_{n-k}\left(mod\ 2^m\right),\ j < k\ . \qquad \textbf{(1.1.13)}$$

Nors šis generatorius turi maksimalų periodą $\left(2^k - 1\right)2^{m-3}$, kuris yra tik ketvirtadalis atitinkamo SVFG, manoma, kad jo empirinės savybės yra geresnės nei SVFG.

Postūmio registrų generatorius (angl. *Shift-Register Generator* (SRG)) yra [20]:

$$x_{n+k} = \sum_{i=0}^{k-1} a_i x_{n+i}\left(mod\ 2\right), \qquad \textbf{(1.1.14)}$$

kur x_n ir a_i yra arba 0 arba 1. Maksimalus periodas $2^k - 1$ pasiekiamas naudojant bent dvi nenulines a_i reikšmes. Yra du būdai kaip gauti atsitiktinius skaičius iš bitų, gautų pagal (1.1.14). Pirmasis, vadinamas skaitmeniniu daugiažingsniu metodu, naudoja *n* einančių vienas paskui kitą bitų iš (1.1.14)

kad suformuoti *n*-bitų sveiką skaičių. Tada dar *n* bitų yra generuojami, kad sukurti sekantį skaičių ir t.t. Antrasis metodas, vadinamas bendriniu grįžtamo ryšio postūmio registru (GFSR), sukuria naują *n*-bitų pseudoatsitiktinį sveiką skaičių kiekvienai (1.1.14) iteracijai. Tai atliekama sudarant *n*-bitų iš paskutinio generuoto bito, x_{n+k}, ir $n-1$ kitų bitų iš *k* bitų iš SRG. Tokiu būdu, kiekvienam naujam bitui generuojamas atsitiktinis skaičius. Nors šie du metodai atrodo skirtingi, jie yra panašūs ir teoriniai rezultatai gauti vienam gali būti pritaikomi kitam. Jei *k* yra mažas, gali atsirasti autokoreliacija.

Tiesinis grįžtamo ryšio postūmio registras (angl. *Linear Feedback Shift Register* - LFSR) gali būti realizuotas techninėje įrangoje. Tai daro jį naudingą ten, kur reikalingi greiti AS generatoriai [17].

LFSR generuotos skaičių sekos gali būti laikomos dvejetainių skaitmenų sistema, tokia kaip Grėjaus kodas, arba paprastas dvejetainis kodas. Tam tikrais taikymo atvejais reikia skirtingom reikšmėm pažymėti taškus išilgai tam tikro atstumo. Pavyzdžiui, dauguma matavimo juostų žymi kiekvieną colį ar centimetrą vienintele reikšme naudodama dešimtainę skaičių sistemą. Kai šie taškai turi būti apdorojami kompiuteriu, jie dažnai žymimi naudojant LFSR seką. Taip daroma, nes LFSR skaitikliai yra paprastesni ir greitesni nei kitų rūšių skaitikliai – greitesni nei paprastas dvejetainis arba Grėjaus skaitikliai.

LFSR ilgą laiką buvo AS generatorius naudojamas informacijos srautams šifruoti, nes buvo lengvai konstruojamas iš elektromechaninių ir elektroninių schemų, turėjo ilgą periodą ir tolygiai pasiskirsčiusius išvesties rezultatus. Kaip bebūtų, LFSR rezultatai yra visiškai tiesiniai, o tai reiškia, kad būtų lengva iššifruoti jais užšifruotą informaciją. Yra įvairūs būdai šio trūkumo pašalinimui: pvz., netiesinė dviejų LFSR išėjimų kombinacija ir t.t.

Pagrindinis atsitiktinių skaičių generatorius

Tai yra vadinamasis daugybos su perpildymu arba rekursijos su perpildymu generatorius (angl. *Mother-of-All*), sugalvotas Džordžo Marsaglos (angl. *George Marsaglia*) [11]. Algoritmas yra toks:

$$S = 2111111111 \cdot X_{n-4} + 1492 \cdot X_{n-3} + 1776 \cdot X_{n-2} + 5115 \cdot X_{n-1} + C,$$

$$X_n = S \left(\mathrm{mod}\, 2^{32}\right),$$

$$C = floor\left(S / 2^{32}\right) \qquad \textbf{(1.1.15)}$$

Paskutinės keturios *X* ir *C* reikšmės saugomos atmintyje kaip 32 bitų neapibrėžto ženklo sveiki skaičiai. Tarpinis rezultatas *S* yra 64 bitų neapibrėžto ženklo sveikas skaičius. *X* ir *S* pradinės reikšmės parenkamos nelygios nuliui. Savybės:

- 32 bitų sveikų skaičių išvestis,
- ciklo ilgis $3 \cdot 10^{47}$,
- labai geras atsitiktinumas.

„Blum Blum Shub“

Blumo Blumo ir Šubo (angl. *Blum Blum Shub* (BBS)) yra AS generatorius, sukurtas Lenoro Blumo, Manuelio Blumo ir Michaelio Šubo 1986 metai. Algoritmas:

$$x_{n+1} = (x_n)^2 \bmod M \qquad \textbf{(1.1.16)}$$

kur $M = pq$ yra dviejų didelių pirminių skaičių sandauga. Abu pirminiai skaičiai *p* ir *q* turėtų būti kongriuentiniai $3 \bmod 4$ (tai garantuoja, kad kiekviena kvadratinė liekana turi vieną kvadratinę šaknį, kuri taip pat yra kvadratinė liekana) ir $DBD(\varphi(p-1), \varphi(q-1))$ (Didžiausias Bendras Daliklis) turėtų būti mažas, nes tai užtikrina ilgą ciklą.

Šis generatorius nėra labai greitas, todėl jis tinkamas kriptografijai, bet ne modeliavimams. Jis yra nepaprastai saugus ir kokybiškas, nes sudėtinga skaidyti sveikus skaičius dauginamaisiais. Atitinkamai parinkus pirminius skaičius, kai $O(\log\log M)$ bitų iš kiekvieno x_n yra išvestis, tada riboje, kai *M* didėja, atskirti išvesties bitus nuo atsitiktinių bus taip pat sudėtinga, kaip išskaidyti *M* dauginamaisiais. Jei sveikų skaičių išskaidymas dauginamaisiais yra sudėtingas, tada BBS su dideliu *M* turės išvestį nepriklausomą nuo neatsitiktinių struktūrų, kurios galėtų būti aptinkamos tam tikrais skaičiavimais. Teoriškai įmanoma, kad kada nors bus sugalvotas greitas skaičių skaidymo dauginamaisiais algoritmas, taigi BBS nėra garantuotai saugus [8,9].

„Mersenne Twister“

Mersenne Twister (MT) yra AS generuojantis algoritmas sukurtas Makoto Matsumoto ir Takujo Nishimuros 1996/1997 metais. Jis skirtas greitai generuoti aukštos kokybės AS. Yra bent du algoritmo atvejai, besiskiriantys naudojamais Mersene pirminiais skaičiais (Mersene pirminis yra pirminis skaičius, kuris yra vienetu mažesnis nei du pakelta laipsniu, kuris irgi yra pirminis skaičius $M_n = 2^n - 1$). Naujesnis ir dažniau naudojas yra MT 19937.

Privalumai:

- sukurtas nagrinėjant kitų egzistuojančių generatorių trūkumus,
- algoritmas suprogramuotas su C,
- žymiai ilgesnis periodas ir žymiai geresnė išsibarstymo tvarka, nei kituose realizuotuose generatoriuose (Įrodyta, kad periodas yra $2^{19937} - 1$, ir 623 matavimų vienodo išsibarstymo savybės yra garantuojamos),
- greita generacija,
- efektyvus atminties naudojimas,

MT sukurtas remiantis praktinių savybių, kurias generatorius turėtų tenkinti, tyrimais. Manoma, kad spekrinis testas yra vienas iš geresnių būdų nustatyti gerą generatorių. MT yra patobulinta

sėkmingo generatoriaus TT800, turinčio periodą $2^{800}-1$, versija. Generatorius sukurtas taip, kad generuotų išvestį tik greičiausiomis aritmetinėmis operacijomis: nėra dalybos ar daugybos.

Pats algoritmas yra susuktas GLFSR. Susukimas yra transformacija, kuri garantuoja vienodą sugeneruotų skaičių pasiskirstymą 623 matavimuose. Priešingai nei BBS, algoritmas savo prigimtimi nėra tinkamas kriptografijai [10].

Generatorių derinys

Naujos, geresnės kokybės sekos gali būti gaunamos maišant išvestis iš keletos žinomų generatorių [15]:

$$z_n = x_n \oplus y_n \qquad \textbf{(1.1.17)}$$

kur $\oplus$ dažniausiai yra išskirtinė ARBA operacija, arba suma moduliu *m*, *x* ir ir *y* yra sekos iš dviejų nepriklausomų generatorių. Geriausia, jei abiejų generatorių ciklo ilgiai yra reliatyviai pirminiai, nes tai reiškia, kad *z* ciklo ilgis bus pagrindinių generatorių ciklo ilgių sandauga. Galima parodyti, kad *z* statistinės savybės nėra blogesnės nei *x* ar *y*.

1.2 ATSITIKTINIŲ DYDŽIŲ SKAITINĖS CHARAKTERISTIKOS

1.2.1 PAGRINDINĖS SĄVOKOS

A1. Atsitiktinis procesas $(\xi_t,\ t \in T)$ yra atsitiktinių dydžių šeima, priklausanti nuo parametro *t* ir apibrėžta tikimybinėje erdvėje (Ω, F, P). Parametro *t* kitimo aibė *T* kartais vadinama indeksų aibe. *t* dažniausiai interpretuojamas kaip laikas. Dažniausiai *T* yra sveikų skaičių aibė $\{\ldots,-1,0,1,\ldots\}$. Tokie atsitiktiniai procesai vadinami diskretaus laiko atsitiktiniais procesais.

A2. Funkcija $m(t) = E\xi_t$ vadinama atsitiktinio proceso ξ_t matematiniu vidurkiu.

A3. Sekos $\{\xi_t,\ t \in T\}$ antros eilės mišrusis momentas vadinamas kovariacine funkcija $R(t,s)$:

$R(t,s) = E\{(\xi_t - m(t))(\xi_s - m(s))\} = \operatorname{cov}(\xi_t, \xi_s)$.

Jei $s = t$, tai $\operatorname{cov}(\xi_t, \xi_s) = D(\xi_t)$ ir žymi atsitiktinio dydžio ξ_t dispersiją.

Jei $R(t,s) \equiv 0$ kiekvienam $s \neq t$, tai $\{\xi_t,\ t \in Z\}$ yra nekoreliuotųjų dydžių seka [2].

A4. Procesas ξ_t vadinamas stacionariu siaurąja prasme, jei jo daugiamačiai pasiskirstymai nepriklauso nuo postūmio laike, t. y. $\forall t_1,\ldots,t_k \in T, k = 1,2,\ldots$

$F_{t_1,\ldots,t_k}(\cdot) = F_{t_1+\tau,\ldots,t_k+\tau}(\cdot)$, jei $t_i + \tau \in T$.

Tai labai griežta salyga, kurią sunku patinkrinti empiriškai.

A5. Procesas ξ_t vadinamas stacionariu plačiąja prasme, jei jo matematinis vidurkis ir kovariacinė funkcija nepriklauso nuo poslinkio laike, t. y. $\forall t,s \in T \quad m(t) = m(0)$ ir $R(t,s) = R(t-s,0)$.

Akivaizdu, kad jei procesas ξ_t tenkina **A4.** ir turi dispersiją, tai jis tenkina ir **A5.**, bet ne atvirkščiai. Tačiau, jei procesas ξ_t yra Gauso, jam abu apibrėžimai sutampa.

Toliau procesas vadinamas stacionariu, jei jis stacionarus plačiąja prasme. Taigi stacionaraus proceso ξ_t matematinis vidurkis nekinta laike $E\xi_t = m$, o kovariacinė funkcija yra vieno argumento funkcija $R(\tau) = \text{cov}(\xi_{t+\tau}, \xi_t)$ visiems $t \in T$ [7].

Kovariacinė funkcija $R(\tau) = \text{cov}(\xi_t, \xi_{t-\tau})$ vadinama τ vėlinimo autokovariacine ξ_t funkcija. Ji turi dvi svarbias savybes: a) $R(0) = D(\xi_t)$; b) $R(-\tau) = R(\tau)$. Antroji savybė yra teisinga, nes: $\text{cov}(\xi_t, \xi_{t-(-\tau)}) = \text{cov}(\xi_{t-(-\tau)}, \xi_t) = \text{cov}(\xi_{t+\tau}, \xi_t) = \text{cov}(\xi_k, \xi_{k-\tau})$, kur $k = t + \tau$.

A6. Atsitiktinis procesas ε_t vadinamas baltu triukšmu, jei $\{\varepsilon_t\}$ yra nepriklausomų ir vienodai pasiskirsčiusių atsitiktinių dydžių seka su baigtiniu vidurkiu ir dispersija. Atskiru atveju, kai ε_t pasiskirstęs pagal Normalųjį dėsnį su vidurkiu lygiu nuliui ir dispersija σ^2, procesas vadinamas Gauso baltu triukšmu. Balto triukšmo savybės:

1) $E\varepsilon_t = 0$;

2) $\text{cov}(\varepsilon_t, \varepsilon_s) = 0$, kai $t \neq s$.

Praktiškai, jei autokoreliacijos funkcija yra artima nuliui, tai procesas yra balto triukšmo procesas [7].

1.2.2 AUTOKORELIACIJOS FUNKCIJA

Koreliacijos koeficientas tarp atsitiktinių dydžių *X* ir *Y* apibrėžiamas taip:

$$r_{X,Y} = \frac{\text{cov}(X,Y)}{\sqrt{D(X)D(Y)}} = \frac{E[(X-EX)(Y-EY)]}{\sqrt{E(X-EX)^2 E(Y-EY)^2}}, \qquad \textbf{(1.2.1)}$$

kur *EX* ir *EY* yra atitinkamai *X* ir *Y* vidurkiai ir priimama kad dispersijos egzistuoja. Šis koeficientas parodo tiesinės priklausomybės tarp *X* ir *Y* stiprumą, taip pat $|r_{X,Y}| \leq 1$ ir $r_{X,Y} = r_{Y,X}$. Du atsitiktiniai dydžiai yra nekoreliuoti, jei $r_{X,Y} = 0$. Be to, jei abu, *X* ir *Y* yra pasiskirstę pagal normalųjį dėsnį, tada $r_{X,Y} = 0$ tada ir tik tada, kai *X* ir *Y* yra nepriklausomi.

Nagrinėjama stacionari diskrečių atsitiktinių dydžių seka ξ_t. Kai domina tiesinė priklausomybė tarp ξ_t ir ξ_{t-i} $\left(i = \overline{0,t}\right)$ koreliacijos sąvoka apibendrinama autokoreliacijai. Koreliacijos koeficientas

tarp ξ_t ir $\xi_{t-\tau}$ vadinamas τ vėlinimo ξ_t autokoreliacija, dažniausiai žymima $r(\tau)$ ir pagal stacionarumo prielaidas yra funkcija priklausanti tik nuo τ. Apibrėžiama taip:

$$r(\tau)=\frac{\operatorname{cov}(\xi_t,\xi_{t-\tau})}{\sqrt{D(\xi_t)D(\xi_{t-\tau})}}=\frac{\operatorname{cov}(\xi_t,\xi_{t-\tau})}{D(\xi_t)}=\frac{R(\tau)}{R(0)}, \qquad \textbf{(1.2.2)}$$

kur panaudota stacionarių sekų savybė: $D(\xi_t)=D(\xi_{t-\tau})$. Čia $r(\tau)$ – autokoreliacijos funkcija, $R(\tau)$ – kovariacinė funkcija. Pagal apibrėžimą turime, kad $r(0)=1$, $r(\tau)=r(-\tau)$ ir $|r(\tau)|\le 1$. Be to, stacionarios sekos yra neautokoreliuotos tada ir tik tada, kai $r(\tau)=0$ visiems $\tau>0$.

Tegul ξ_t yra stacionarus procesas su kovariacine funkcija $R(\tau)$. Turimi stebėjimai $\xi_1,...,\xi_n$. Kai nesinaudojama apriorine informacija apie įvertinamų funkcijų pavidalą, taikomas neparametrinis įvertinimas. Kadangi $R(\tau)=E(\xi_{t+\tau}-m)(\xi_t-m)$, tai:

$$\hat{R}(\tau)=\frac{1}{n-|\tau|}\sum_{t=1}^{n-|\tau|}(\xi_{t+|\tau|}-m)(\xi_t-m) \qquad \textbf{(1.2.3)}$$

Šis įvertis yra nepaslinktas, bet jei vidurkis *m* nėra žinomas, jis keičiamas į $\hat{m}=\frac{\xi_1+...+\xi_n}{n}$, o nepaslinktas įvertis yra:

$$\hat{R}=\frac{1}{n-|\tau|-1}\sum_{t=1}^{n-|\tau|}(\xi_{t+|\tau|}-\hat{m})(\xi_t-\hat{m}).$$

Tačiau dažniausiai vartojamas asimptotiškai nepaslinktas įvertis:

$$\hat{R}=\frac{1}{n}\sum_{t=1}^{n-|\tau|}(\xi_{t+|\tau|}-\hat{m})(\xi_t-\hat{m}). \qquad \textbf{(1.2.4)}$$

Toliau $\hat{R}(\tau)$ bus žymimas asimptotiškai nepaslinktas įvertį (1.2.4), kuris turi mažesnę dispersiją nei (1.2.3), jis dar vadinamas empirine kovariacine funkcija. Aišku, kad $\hat{R}(\tau)$=0, kai $|\tau|\ge n$.

Sekos ξ_t su vėlinimu τ autokoreliacijos funkcijos įvertis apibrėžiamas taip:

$$\hat{r}(\tau)=\frac{\sum_{t=\tau+1}^{T}(\xi_t-m)(\xi_{t-\tau}-m)}{\sum_{t=1}^{T}(\xi_t-m)^2},\quad 0\le\tau<T-1. \qquad \textbf{(1.2.5)}$$

1.2.3 SPEKTRINIS TANKIS

Visiškai kitokia analizės rūšis yra spektrinė laiko eilučių analizė. Ji pagrįsta faktu, kad diskretaus laiko stacionarios eilutės ξ_t kovariacinė funkcija $R(\tau)$ turi atvirkštinę Furjė transformaciją. Tiriant procesus naudojama dažnuminė analizė, todėl svarbiomis charakteristikomis yra spektrinė funkcija ir spektrinis tankis.

Matematikoje, diskrečioji Furjė transformacija (DFT), kartais dar vadinama baigtine Furjė transformacija (BFT) dažnai naudojama signalų apdorojime ir panašiose srityse. DFT gali būti paskaičiuojama naudojantis greita Furjė transformacija (GFT) [12].

Proceso spektrinis tankis egzistuoja tada ir tik tada, kai procesas yra stacionarus. Jei procesas nėra stacionarus, tai algoritmas, naudojamas skaičiuoti spektriniam tankiui gali būti naudojamas, bet rezultatas negalės būti vadinamas spektriniu tankiu. Stacionariems procesams, spektrinis tankis yra avirkštinė kovariacinės funkcijos Furjė transformacija:

$$h(\lambda)=\frac{1}{N}\sum_{\tau=0}^{N-1}R(\tau)e^{\frac{2\pi i}{N}\tau\lambda},\ \lambda=0,...,N-1, \qquad \textbf{(1.2.6)}$$

$$R(\tau)=\sum_{\lambda=0}^{N-1}h(\lambda)e^{-\frac{2\pi i}{N}\tau\lambda},\ \tau=0,...,N-1, \qquad \textbf{(1.2.7)}$$

o kovariacinė funkcija – tiesioginė spektrinio tankio Furjė transformacija:

kur $h(\lambda)$ - spektrinis tankis. Jis parodo, kaip pasiskirsčiusi proceso nešama energija pagal dažnumus. Spektrinis tankis ir kovariacinė funkcija formuoja Furjė transformacijų porą [13].

Skaičiuojant proceso GFT, gaunamas proceso spektras, parodantis, kaip pasiskirsčiusios proceso reikšmės pagal dažnį.

1.2.4 SKIRSTINIŲ KEITIMAS

Sprendžiant beveik kiekvieną praktinį tikimybių teorijos ar matematinės statistikos uždavinį tenka naudotis tam tikrų atsitiktinių dydžių pasiskirstymo funkcijų arba kvantilių reikšmėmis. Tolygusis skirstinys $T(0,1)$ dažnai taikomas matematinėje statistikoje, nes pasižymi tokia svarbia savybe: jeigu X yra tolydusis atsitiktinis dydis, kurio pasiskirstymo funkcija $F(x)$, tai atsitiktinis dydis $Y=F(X)$ bus tolygiai pasiskirstęs intervale $(0,1)$, t.y. $Y\sim T(0,1)$ [3]. Iš tikrųjų

$$P\{Y<y\}=P\{F(x)<y\}=P\{X<F^{-1}(y)\}=F(F^{-1}(y))=y. \qquad \textbf{(1.2.8)}$$

1.2.5 PIRSONO χ^2 SUDERINAMUMO KRITERIJUS

Paprastąja neparametrine hipoteze vadinama prielaida apie tikimybių skirstinio analizinę išraišką. Kriterijai, kuriais remiantis tikrinamos paprastosios neparametrinės hipotezės vadinami suderinamumo kriterijais. Nagrinėjamas Pirsono χ^2 kriterijus [1]. Šis suderinamumo kriterijus yra universalus.

Sakykime, $(X_1, X_2, \ldots, X_n)$ yra atsitiktinio dydžio X su nežinoma pasiskirstymo funkcija $F(x)$ atsitiktinė imtis. Tikrinama paprastoji hipotezė $H_0: F(x)=F_0(x)$. Visa dydžio X galimų

reikšmių aibė skaidoma į *m* intervalų. Tarus, kad H_0 yra teisinga, apskaičiuojamos teorinės tikimybės p_i. Teorinės ir empirinės pasiskirstymo funkcijos nuokrypio matu imama statistika:

$$\mathbf{X_n^2} = \sum_{i=1}^{m} \frac{(k_i - np_i)^2}{np_i}, \qquad \textbf{(1.2.9)}$$

kur k_i – stebėtas reikšmių pakliuvusių į *i*-ajį intervalą skaičius; np_i – tikėtasis reikšmių pakliuvusių į *i*-ajį intervalą skaičius; *m* – intervalų skaičius.

Jei hipotezė H_0 yra teisinga, statistika $\mathbf{X_n^2}$ yra asimptotiškai $(n \to \infty)$ pasiskirsčiusi pagal χ^2 dėsnį su $m-1$ laisvės laipsniais. Jei statistikos $\mathbf{X_n^2}$ konkreti reikšmė $x_n^2 \geq \chi_p^2(m-1)$, hipotezė H_0 atmetama, jei $x_n^2 < \chi_p^2(m-1)$, H_0 priimama.

1.2.6 PORTMANTEAU TESTAS

Įvairiems matematiniams taikymams dažnai reikia patikrinti, kad tam tikra autokoreliacijos funkcijos reikšmių aibė yra lygi nuliui. Boksas ir Piersas (angl. *Box, Pierce*) (1970) pasiūlė Portmanteau statistiką [6]:

$$Q^*(m) = T\sum_{i=1}^{m} \hat{r}_i^2(\tau) \qquad \textbf{(1.2.14)}$$

kaip nulinės hipotezės $H_0 : r_1(\tau) = \ldots = r_m(\tau) = 0$ prie alternatyvos $H_a : r_i(\tau) \neq 0$ su tam tikrais $i \in \{1, ..., m\}$ tikrinimo statistiką. Tarus, kad $\{\xi_t, t \in T\}$ yra nepriklausomų, vienodai pasiskirsčiusių dydžių seka, $Q^*(m)$ asimptotiškai yra pasiskirstęs pagal χ^2 dėsnį su *m* laisvės laipsniais.

Ljungas ir Boksas (angl. *Ljung, Box*) (1978) pakeitė $Q^*(m)$ statistiką, tam kad būtų padidintas testo galiojimas baigtinėms imtims

$$Q(m) = T(T+2)\sum_{i=1}^{m} \frac{\hat{r}_i^2(\tau)}{T-i}. \qquad \textbf{(1.2.15)}$$

m pasirinkimas gali įtakoti $Q(m)$ statistikos veikimą. Ljungo Bokso statistika tikrinama jungtinė nulinė hipotezė, jog procesas yra neautokoreliuotas iki pasirinkto vėlavimo. Dažniausiai siūloma rinktis $m \approx \ln(T)$.

1.3 PROGRAMINĖS ĮRANGOS PASIRINKIMO ANALIZĖ

Pasaulyje yra sukurta nemažai programinės įrangos. Dažnai ši gausa apsunkina pasirinkimą. Galima naudotis universaliomis programavimo kalbomis (FORTRAN, DELPHI, C++, JAVA ir t.t.), universaliais matematiniais paketais (MATLAB, MATHCAD, MATEMATICA ir t.t.). Duomenų analizei geriausia naudoti duomenų analizės sistemas (SAS, STATISTIKA, SPSS, ir t.t.).

Šiame darbe naudojama MATLAB 6 versiją [4]. Šio programinės įrangos paketo pasirinkimą lėmė tai, kad yra nemažai literatūros su programų pavydžiais. Taip pat jame yra realizuota nemažai specialių matematinių funkcijų, o tai palengvino programos kūrimą. Nesunku buvo kurti grafinę vartotojo sąsają. Šis programinis paketas turi tik vieną trūkumą: jame nėra įdiegti kai kurie lietuvių kalbos simboliai (balsės su nosinėmis ir pan.).

Taip pat šiame darbe panaudojamas statistinis paketas SAS. Juo buvo apskaičiuotos geriausios (determinacijos koeficiento R^2 prasme) tranformacijų funkcijų išraiškos.

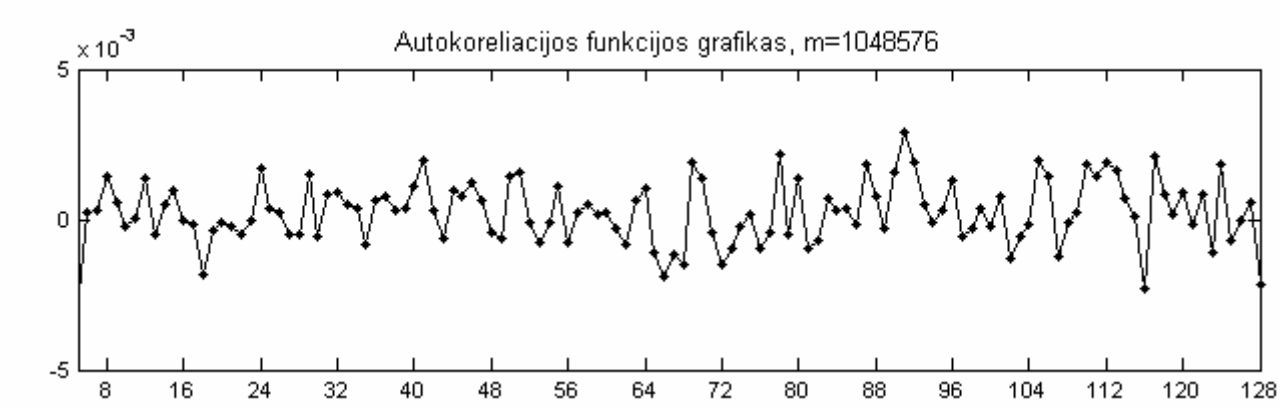
2. TIRIAMOJI DALIS

2.1 TIESINIO KONGRIUENTINIO GENERATORIAUS TYRIMAS

Nagrinėjamas tiesinis kongriunetinis generatorius.

$$x_{n+1} = (9301x_n + 49297) \bmod 233280 . \qquad \textbf{(2.1)}$$

Pagal (1.2.5) skaičiuojama ir braižoma atsitiktinio proceso autokoreliacijos funkcija su vėlavimu $\tau = 0,...,128$ (braižoma su vėlinimu $\tau = 5,...,128$, tam kad esant didelėms pirmosioms reikšmėms, grafiko mastelis nepasikeistų ir būtų matomas funkcijos kitimas) (**2.1 pav).**



2.1 pav. Atsitiktinio proceso autokoreliacijos funkcijos grafikas

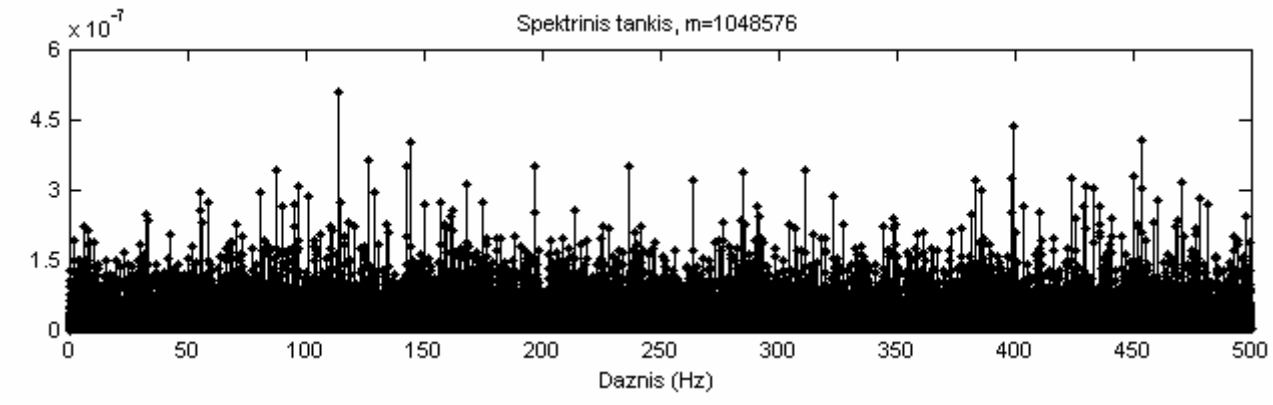
Bokso ir Ljungo statistika (1.2.15) tikrinama jungtinė nulinė hipotezė apie autokoreliacijos funkcijos lygybę nuliui iki pasirinkto vėlavimo (šiuo atveju vėlavimas $\tau = m - 1$), kur *m* yra generuotų AS skaičius. **2.1 lentelėje** pateikta vidutinė (imtis buvo generuota 10 kartų) statistikos reikšmė ir sprendimas (H_0 atmetama arba neatmetama).

2.1 lentelė

Vidutinės Bokso Ljungo statistikos reikšmės

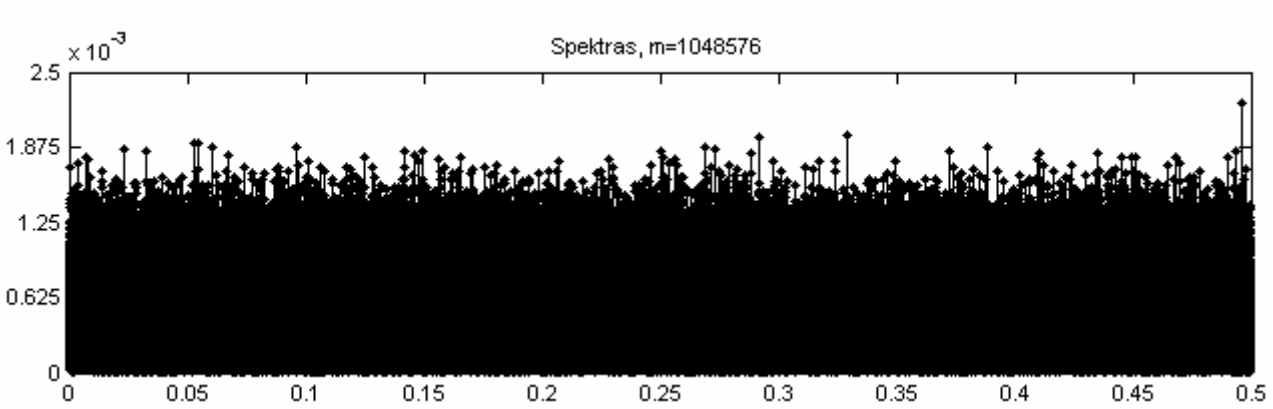
m	Vidutinė statistikos reikšmė	Sprendimas
1024 x 1024	$1048220 < 1051000$	H_0 neatmetama

Daroma prielaida, kad atsitiktinis procesas yra stacionarus ir skaičiuojant autokoreliacijos funkcijos tiesioginę Furjė transformaciją pagal (1.2.6), gaunamas spektrinis tankis. Braižomas jo grafikas (**2.2 pav.**):



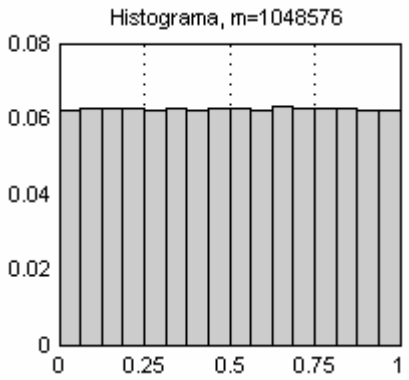
2.2 pav. Atsitiktinio proceso spektrinis tankis

Skaičiuojant atsitiktinio proceso GFT gaunamas atsitiktinio proceso spektras, parodantis atsitiktinio proceso (kaip signalo) pasiskirstymą pagal dažnį. Braižomas jo grafikas (**2.3 pav.**):



2.3 pav. Atsitiktinio proceso spektras

Skaičiuojama ir braižoma santykinių dažnių histograma **2.4 pav.**



2.4 pav. Generuotų AS santykinių dažnių histograma

Pirsono χ^2 suderinamumo kriterijumi tikrinama ar pradiniai AS yra pasiskirstę pagal tolygųjį skirstinį. **2.2 lentelėje** pateikiama vidutinė statistikos reikšmė ir sprendimas (H_0 atmetama arba neatmetama). Kritinė reikšmė - $\chi^2_{0.95}(15) = 25$ [1].

2.2 lentelė

Vidutinės Pirsono χ^2 statistikos reikšmės

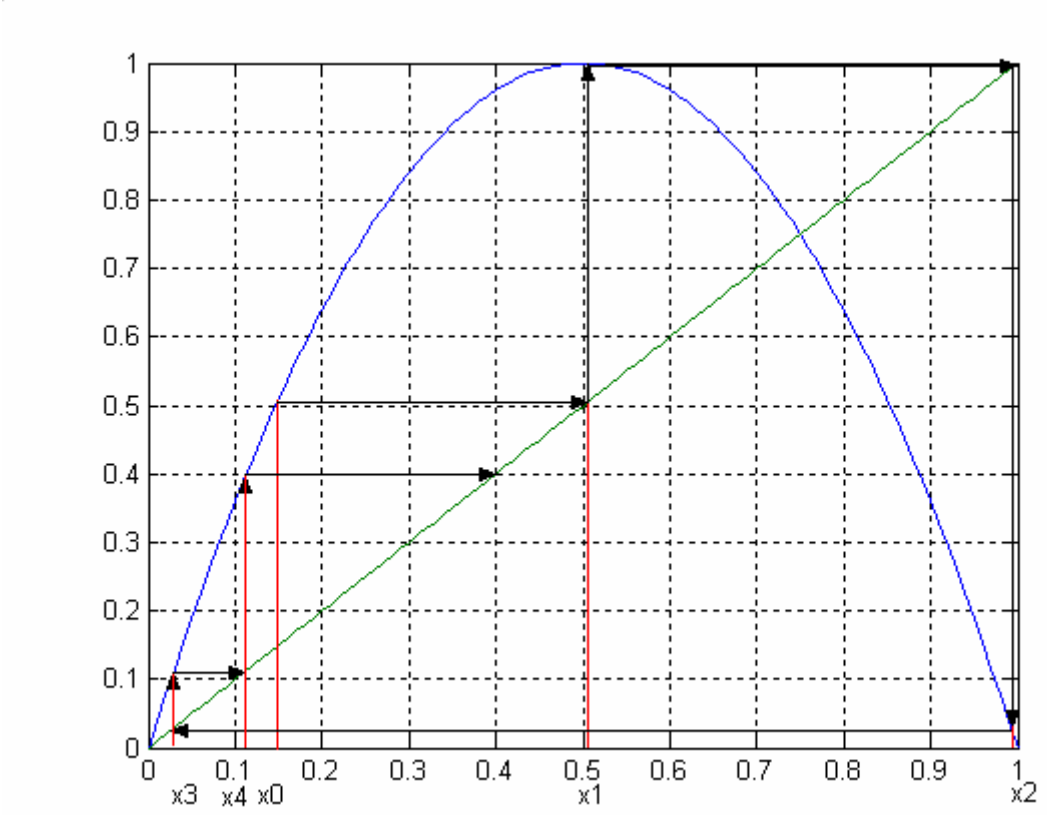
m	Vidutinė statistikos reikšmė	Sprendimas
1024 x 1024	13.9748	H_0 neatmetama

2.2 NETIESINIO KONGRIUENTINIO GENERATORIAUS TYRIMAS

Nagrinėjamas netiesinis kongriuentinis generatorius:

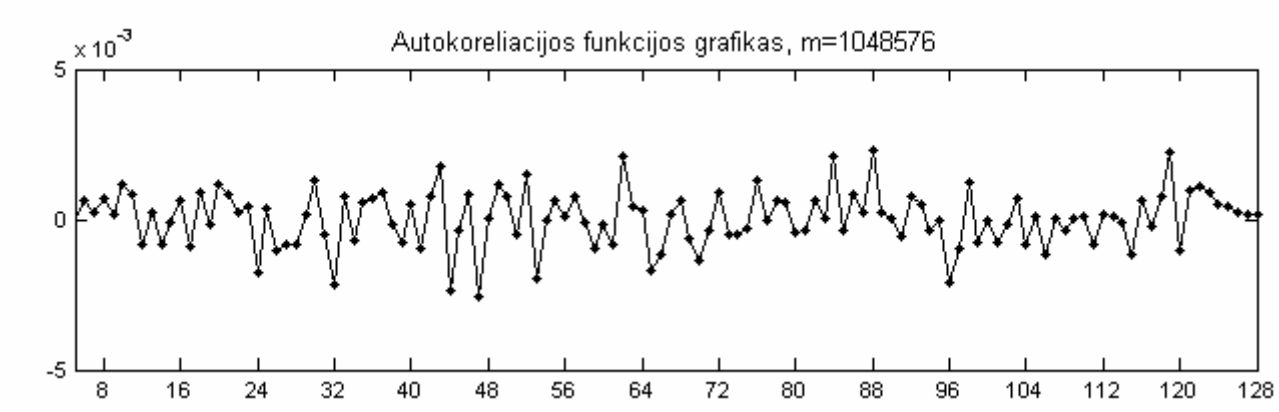
$$x_{i+1} = -4x_i^2 + 4x_i . \qquad \textbf{(2.2)}$$

Reikšmių gavimas pateikiamas **2.5 pav.**



2.5 pav. Reikšmių generavimo algoritmas

Pagal (1.2.5) skaičiuojama ir braižoma atsitiktinių dydžių autokoreliacijos funkcija su vėlavimu $\tau = 0,...,128$ (braižoma su vėlinimu $\tau = 5,...,128$, tam kad esant didelėms pirmosioms reikšmėms, grafiko mastelis nepasikeistų ir būtų matomas funkcijos kitimas) (**2.6 pav).**



2.6 pav. Atsitiktinio proceso autokoreliacijos funkcijos grafikas

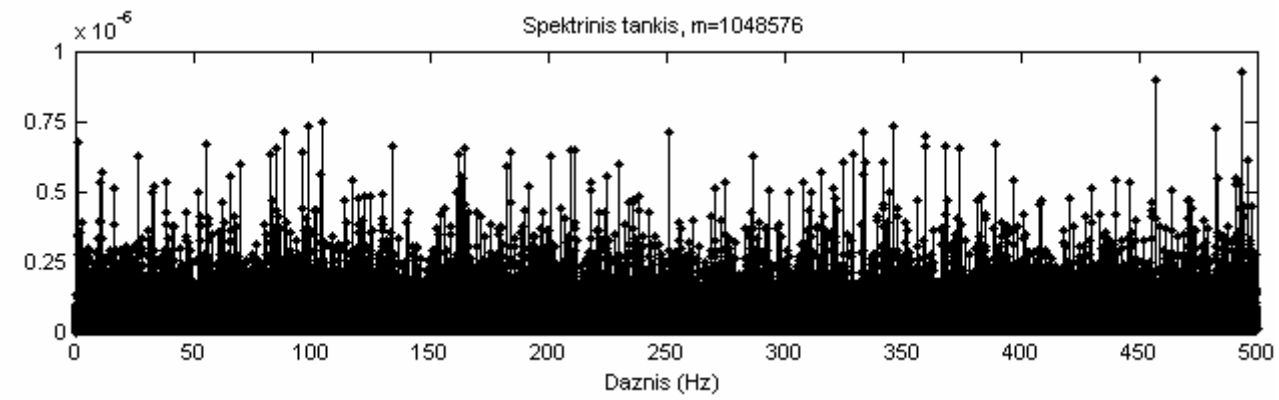
Bokso ir Ljungo statistika (1.2.15) tikrinama jungtinė nulinė hipotezė apie autokoreliacijos funkcijos lygybę nuliui iki pasirinkto vėlavimo (šiuo atveju vėlavimas $\tau = m - 1$), kur *m* yra generuotų AS skaičius. **2.3 lentelėje** pateikiamos vidutinės (kiekvienai *m* reikšmei imtis buvo generuota po 20 kartų) statistikos reikšmės ir sprendimas (H_0 atmetama arba neatmetama).

2.3 lentelė

Vidutinės Bokso Ljungo statistikos reikšmės

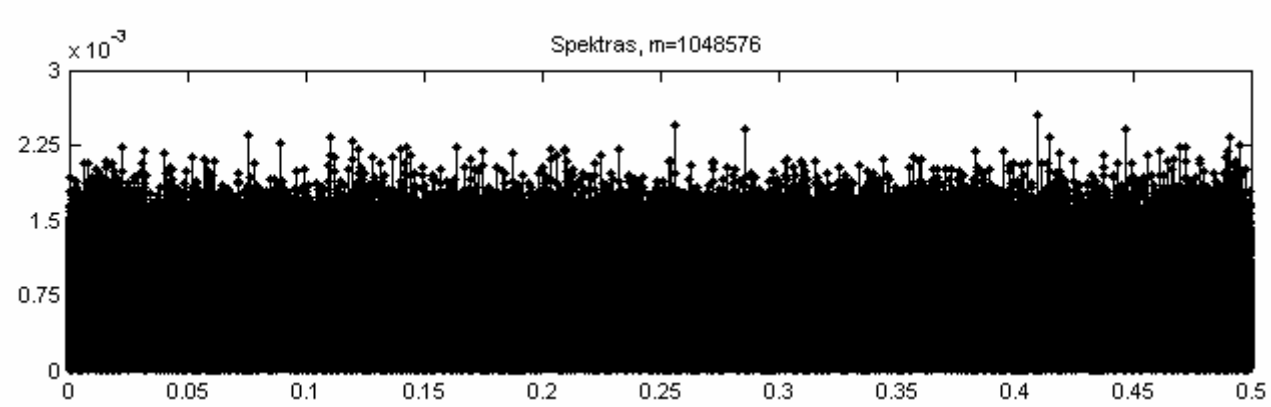
m	Vidutinė statistikos reikšmė	Sprendimas
1024 x 128	$131053 < 131910$	H_0 neatmetama
1024 x 256	$262038 < 263340$	H_0 neatmetama
1024 x 512	$524592 < 525970$	H_0 neatmetama
1024 x 1024	$1049515 < 1051000$	H_0 neatmetama

Daroma prielaida, kad atsitiktinis procesas yra stacionarus ir skaičiuojant autokoreliacijos funkcijos tiesioginę Furjė transformaciją pagal (1.2.6), gaunamas spektrinis tankis. Braižomas jo grafikas (**2.7 pav.**):



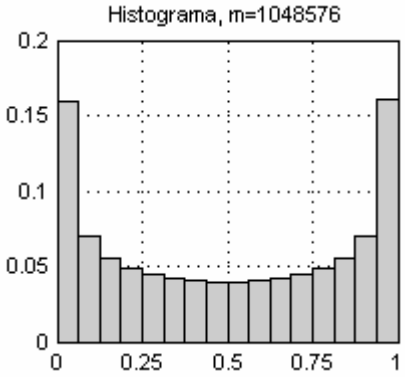
2.7 pav. Atsitiktinio proceso spektrinis tankis

Skaičiuojant atsitiktinio proceso GFT gaunamas atsitiktinio proceso spektras, parodantis atsitiktinio proceso (kaip signalo) pasiskirstymą pagal dažnį. Braižomas jo grafikas (**2.8 pav.**):



2.8 pav. Atsitiktinio proceso spektras

Skaičiuojama ir braižoma santykinių dažnių histograma **2.9 pav.**



2.9 pav. Generuotų AS santykinių dažnių histograma

Pirsono χ^2 suderinamumo kriterijumi tikrinama ar pradiniai AS yra pasiskirstę pagal tolygųjį skirstinį. **2.4 lentelėje** palyginimui pateikiamos vidutinės statistikos reikšmės ir sprendimai (H_0 atmetama arba neatmetama). Kritinė reikšmė - $\chi^2_{0.95}(15) = 25$ [1].

2.4 lentelė

Vidutinės Pirsono χ^2 statistikos reikšmės

m	Vidutinė statistikos reikšmė	Sprendimas
1024 x 128	49428	H_0 atmetama
1024 x 256	98544	H_0 atmetama
1024 x 512	196946	H_0 atmetama
1024 x 1024	393552	H_0 atmetama

AS histograma nėra tolygi, todėl bandymų keliu nustatomas tinkamiausias tankio funkcijos pavidalas, randama pasiskirstymo funkcija ir AS transformuojami. Pagal histogramos pavidalą nagrinėjimui pasirenkamos dvi funkcijos: arksinusas ir parabolė.

Arksinuso tankio funkcija bendru atveju užrašoma taip [3]:

$$p(x)=\begin{cases}0, & \text{kai } x\le -a,\\ \dfrac{1}{\pi\sqrt{a^2-x^2}}, & \text{kai } -a<x<a,\\ 0, & \text{kai } x\ge a.\end{cases}$$

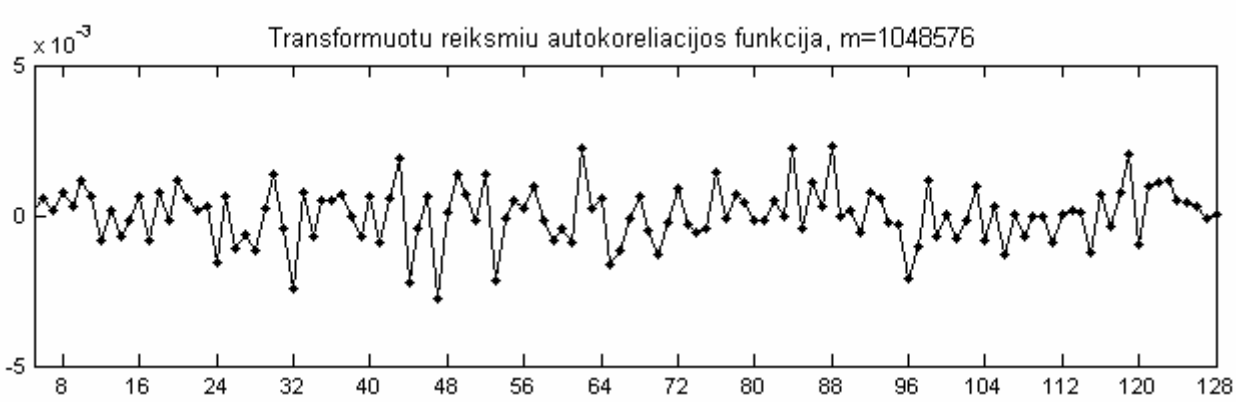
Pasirenkama $a=0.5$, o x paslenkamas, todėl gaunama:

$$p(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{1}{\pi\sqrt{0.5^2-(x-0.5)^2}}, & \text{kai } 0<x<1,\\ 0, & \text{kai } x\ge 1.\end{cases}$$

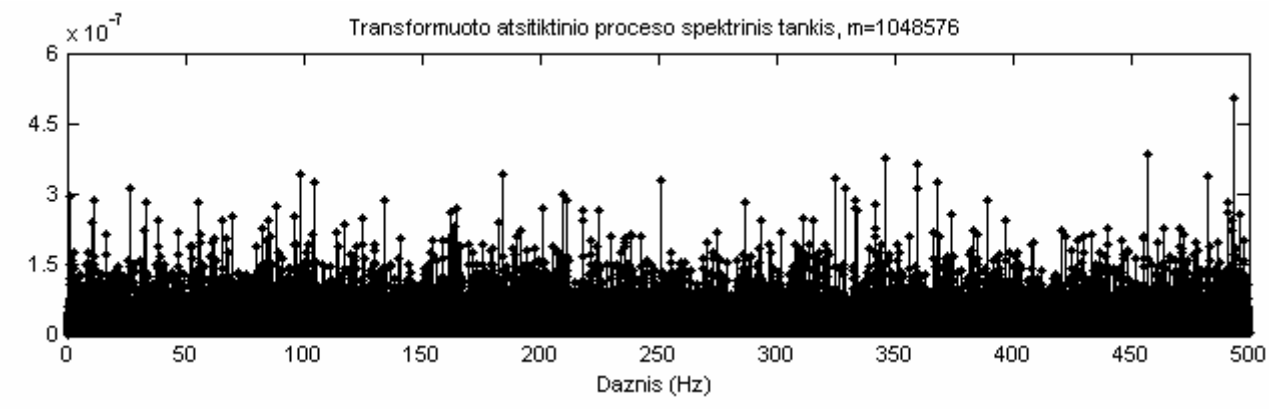
Randama pasiskirstymo funkcija:

$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{1}{\pi}\arcsin\dfrac{x-0.5}{0.5}+\dfrac{1}{2}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases} \qquad \textbf{(2.3)}$$

AS transformuojami, statant juos į analizinę funkcijos išraišką (2.3). Skaičiuojama ir braižoma autokoreliacijos funkcija ir spektrinis tankis (**2.10-2.11 pav.**).

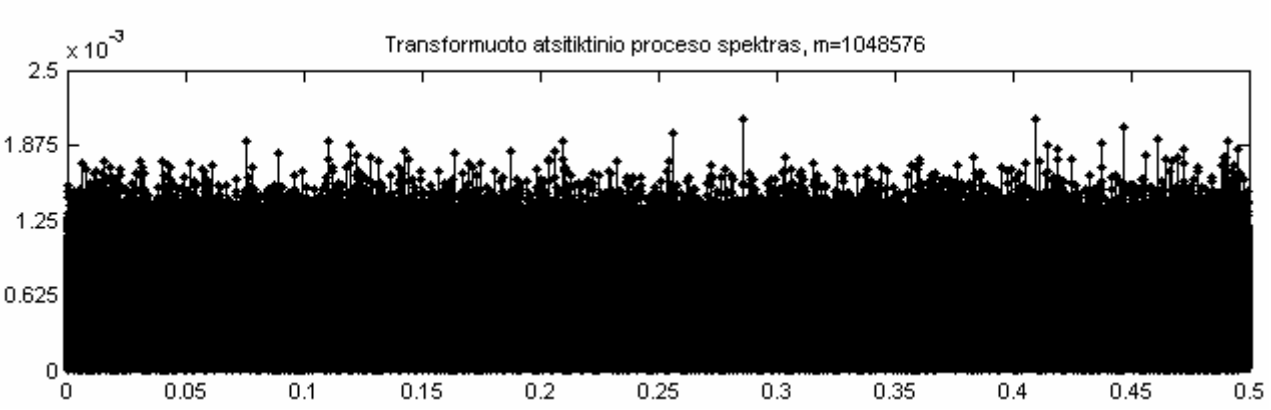


2.10 pav. Transformuot atsitiktinio proceso autokoreliacijos funkcijos grafikas



2.11 pav. Transformuoto atsitiktinio proceso spektrinis tankis

Skaičiuojamas transformuoto atsitiktinio proceso spektras. Braižomas jo grafikas (**2.12 pav.**):



2.12 pav. Transformuoto atsitiktinio proceso spektras

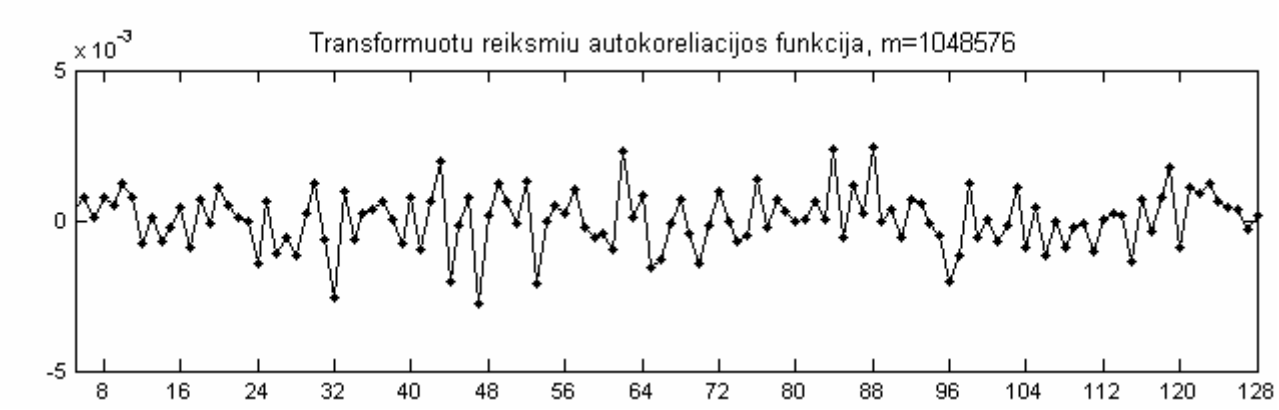
Histograma aproksimuojama parabole. Mažiausių kvadratų metodu gaunama tokia tankio funkcijos išraiška:

$$p(x)=\begin{cases}0, & \text{kai } x\le 0,\\ 0.22820x^2-0.22820x+0.06930, & \text{kai } 0<x<1,\\ 0, & \text{kai } x\ge 1.\end{cases}$$

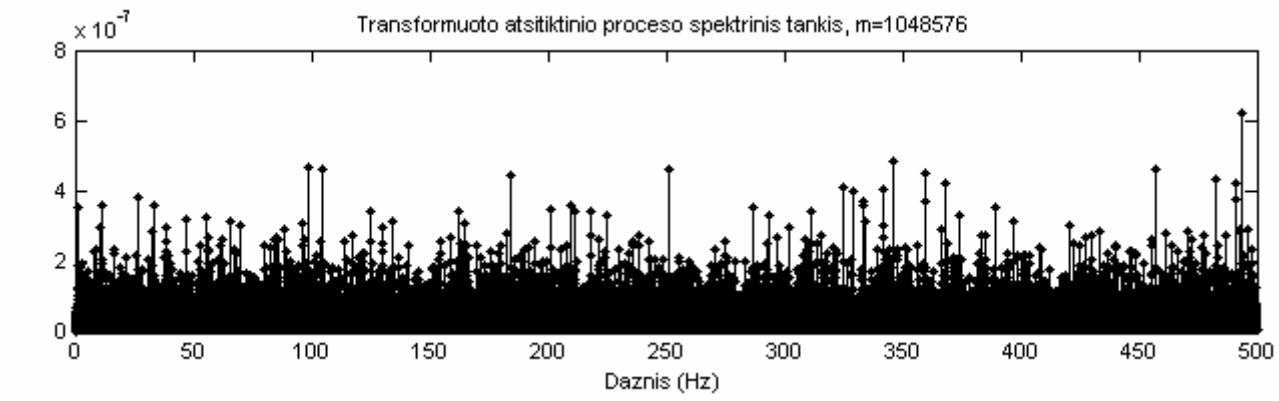
Randama pasiskirstymo funkcija:

$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.22820}{3}x^3-\frac{0.22820}{2}x^2+0.06930x}{\frac{0.22820}{3}-\frac{0.22820}{2}+0.06930}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases} \qquad \textbf{(2.4)}$$

AS transformuojami, statant juos į analizinę funkcijos išraišką (2.4). Skaičiuojama ir braižoma autokoreliacijos funkcija ir spektrinis tankis (**2.13-2.14 pav.**).

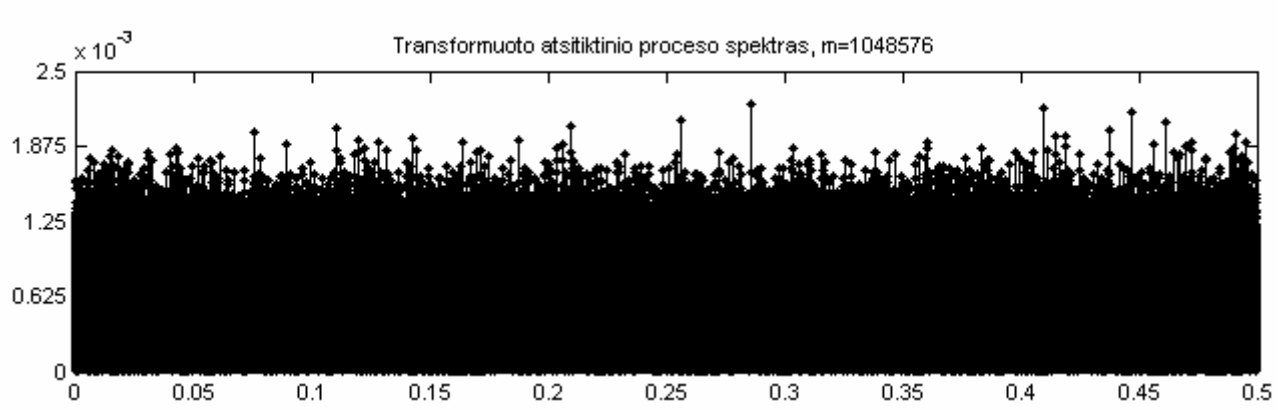


2.13 pav. Transformuoto atsitiktinio proceso autokoreliacijos funkcijos grafikas



2.14 pav. Transformuoto atsitiktinio proceso spektrinis tankis

Skaičiuojamas transformuoto atsitiktinio proceso spektras. Braižomas jo grafikas (**2.15 pav.**):



2.15 pav. Transformuoto atsitiktinio proceso spektras

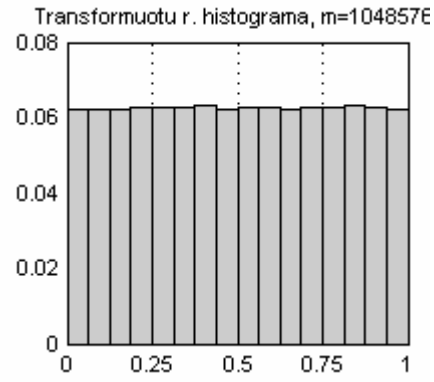
Tikrinamos abiem būdais transformuotų atsitiktinių procesų autokoreliacijos funkcijų lygybės nuliui. **2.5 lentelėje** palyginimui pateikiamos vidutinės (kiekvienai *m* reikšmei imtis buvo generuota po 10 kartų) statistikos reikšmės ir sprendimai (H_0 atmetama arba neatmetama).

2.5 lentelė

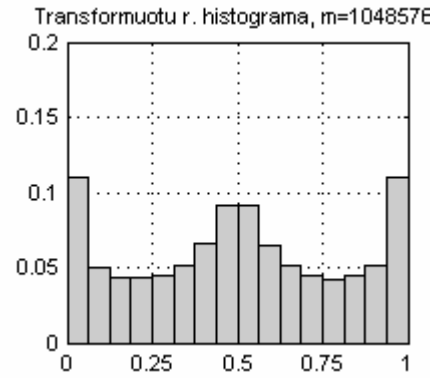
Vidutinės Bokso Ljungo statistikos reikšmės

m	Transformacija – Arksinusas		Transformacija - Parabolė	
	Statistikos reikšmė	Sprendimas	Statistikos reikšmė	Sprendimas
1024 x 128	$131108 < 131910$	H_0 neatmetama	$131146 < 131910$	H_0 neatmetama
1024 x 256	$261627 < 263340$	H_0 neatmetama	$262351 < 263340$	H_0 neatmetama
1024 x 512	$525134 < 525970$	H_0 neatmetama	$524622 < 525970$	H_0 neatmetama
1024 x 1024	$1049490 < 1051000$	H_0 neatmetama	$1050070 < 1051000$	H_0 neatmetama

Skaičiuojamos ir braižomos transformuotų AS santykinių dažnių histogramos (**2.16-2.17 pav.**):



2.16 pav. Transformuotų arksinusu AS santykinių dažnių histograma



2.17 pav. Transformuotų parabole AS santykinių dažnių histograma

Pirsono χ^2 suderinamumo kriterijumi tikrinama ar transformuoti AS yra pasiskirstę pagal tolygųjį skirstinį. **2.6 lentelėje** palyginimui pateikiamos vidutinės statistikos reikšmės ir sprendimai (H_0 atmetama arba neatmetama). Kritinė reikšmė - $\chi^2_{0.95}(15) = 25$ [1].

2.6 lentelė

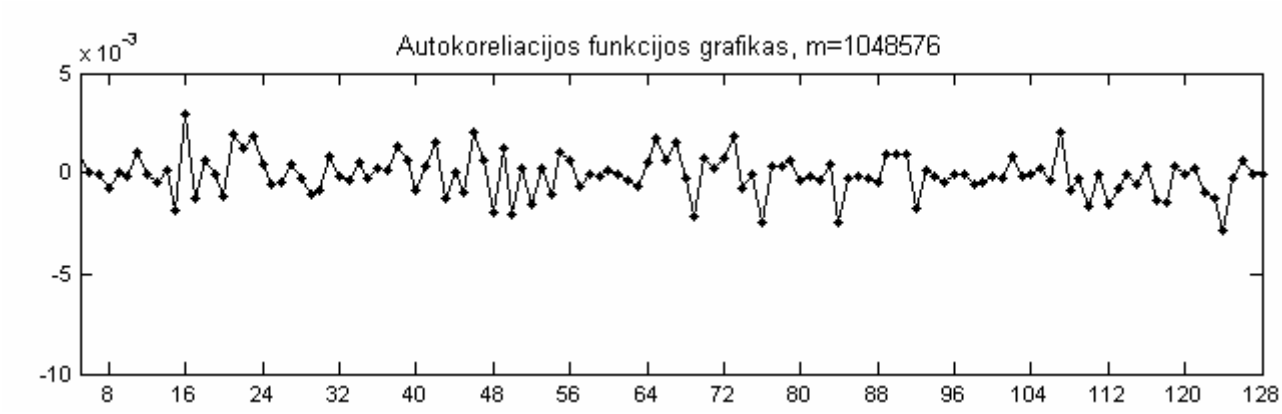
Vidutinės Pirsono χ^2 statistikos reikšmės

m	Transformacija - Arksinusas		Transformacija - Parabolė	
	Statistikos reikšmė	Sprendimas	Statistikos reikšmė	Sprendimas
1024 x 128	11,3	H_0 neatmetama	49482	H_0 atmetama
1024 x 256	11,9	H_0 neatmetama	37517	H_0 atmetama
1024 x 512	15,4	H_0 neatmetama	75132	H_0 atmetama
1024 x 1024	14,0	H_0 neatmetama	150126	H_0 atmetama

2.3 TIESINIO IR NETIESINIO KONGRIUENTINIŲ GENERATORIŲ KOMBINACIJŲ TYRIMAS

Nagrinėjamos 8 tiesinio ir netiesinio kongriuentinių generatorių kombinacijos: v1-v8.

Skaičiuojamos ir braižomos atsitiktinių procesų autokoreliacijos funkcijos su vėlinimu $\tau = 0,...,128$ (braižoma su vėlinimu $\tau = 5,...,128$, tam kad esant didelėms pirmosioms reikšmėms, grafiko mastelis nepasikeistų ir būtų matomas funkcijos kitimas). **2.18 pav.** pateikiamas v1 generatoriaus autokoreliacijos funkcijos grafikas. Visų kombinacijų grafikai pateikiami **1 priede 1 lentelėje**.



2.18 pav. Kombinacijos v1 autokoreliacijos funkcijos grafikas

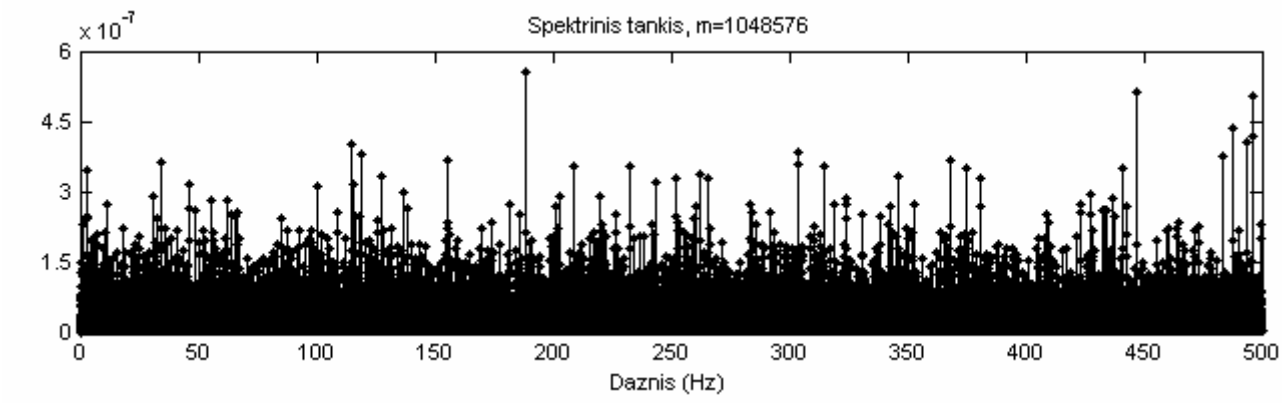
Bokso ir Ljungo statistika (1.2.15) tikrinamos autokoreliacijos funkcijų lygybės nuliui iki vėlavimo $\tau = m - 1$, kur m yra generuotų AS skaičius. **2.7 lentelėje** pateikiamos vidutinės statistikos reikšmės kiekvienai kombinacijai ir sprendimas (H_0 atmetama arba neatmetama).

2.7 lentelė

Vidutinės Bokso Ljungo statistikos reikšmės

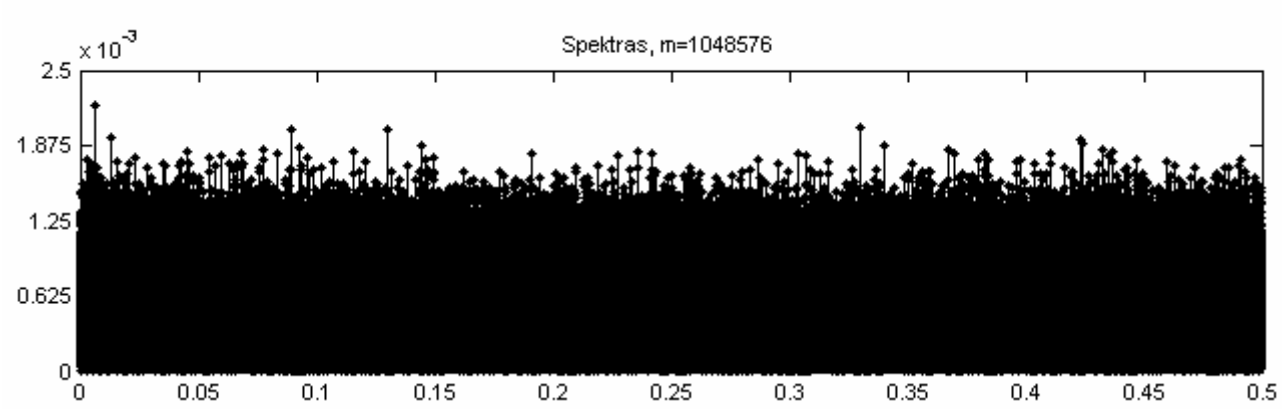
Kombinacija	Vidutinė statistikos reikšmė	Sprendimas
v1	$1049940 < 1051000$	H_0 neatmetama
v2	$1051875 > 1051000$	H_0 atmetama
v3	$1089525 > 1051000$	H_0 atmetama
v4	$1067490 > 1051000$	H_0 atmetama
v5	$1049560 < 1051000$	H_0 neatmetama
v6	$1050295 < 1051000$	H_0 neatmetama
v7	$1068735 > 1051000$	H_0 atmetama
v8	$1089010 > 1051000$	H_0 atmetama

Daroma prielaida, kad atsitiktiniai procesai yra stacionarūs, ir skaičiuojant autokoreliacijos funkcijos tiesioginę Furjė transformaciją pagal (1.2.6), gaunami spektriniai tankiai. Braižomas kombinacijos v1 grafikas (**2.19 pav.**). Visų kombinacijų spektrinių tankių grafikai pateikiami **1 priede 2 lentelėje**.



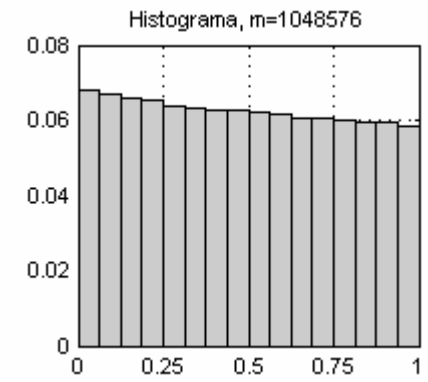
2.19 pav. Atsitiktinio proceso (v1) spektrinis tankis

Skaičiuojant atsitiktinio proceso GFT gaunamas atsitiktinio proceso spektras, parodantis atsitiktinio proceso (kaip signalo) pasiskirstymą pagal dažnį. Braižomas jo grafikas (**2.20 pav.**). Visų kombinacijų spektrų grafikai pateikiami **1 priede 3 lentelėje**.



2.20 pav. Atsitiktinio proceso (v1) spektras

Skaičiuojamos ir braižomos santykinių dažnių histogramos **2.21 pav.** Visų kombinacijų histogramos pateikiamos **1 priede 4 lentelėje**.



2.21 pav. Kombinacijos v1 santykinių dažnių histograma

Pirsono χ^2 suderinamumo kriterijumi tikrinama ar pradiniai AS yra pasiskirstę pagal tolygųjį skirstinį. **2.8 lentelėje** palyginimui pateikiamos vidutinės statistikos reikšmės ir sprendimai (H_0 atmetama arba neatmetama). Kritinė reikšmė - $\chi^2_{0.95}(15) = 25$ [1].

2.8 lentelė

Vidutinės Pirsono χ^2 statistikos reikšmės

Kombinacija	Vidutinė statistikos reikšmė	Sprendimas
v1	2083	H_0 atmetama
v2	2881	H_0 atmetama
v3	4351	H_0 atmetama
v4	1570	H_0 atmetama
v5	2908	H_0 atmetama
v6	2086	H_0 atmetama
v7	1584	H_0 atmetama
v8	4215	H_0 atmetama

AS histogramos nėra tolygios, todėl bandymų keliu nustatomi tinkamiausi tankio funkcijų pavidalai, randamos pasiskirstymo funkcijos ir AS transformuojami. Pagal histogramos pavidalus nagrinėjimui pasirenkamos dvi funkcijos: tiesė ir parabolė.

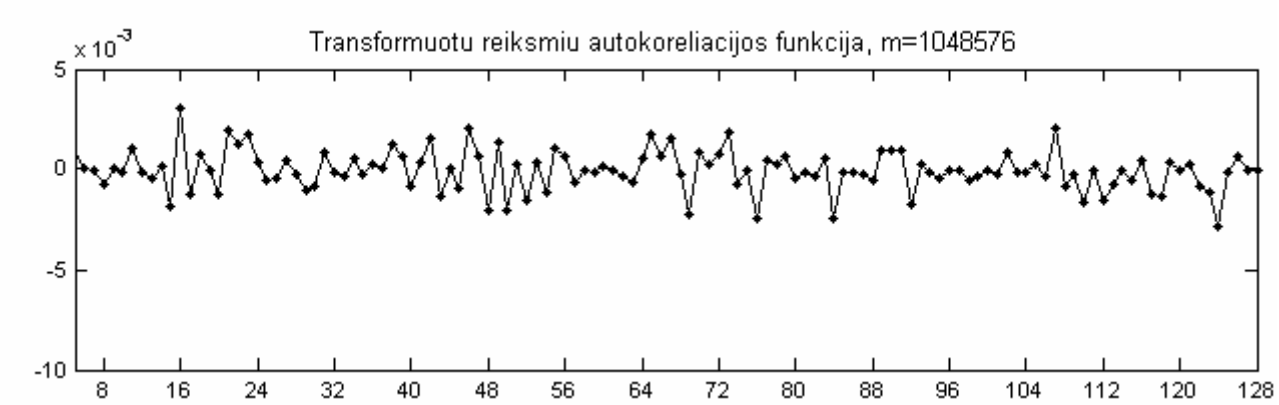
Histograma aproksimuojama tiese. Mažiausių kvadratų metodu kombinacijai v1 gaunama tokia tankio funkcijos išraiška (visos transformacijom reikalingos funkcijų išraiškos pateikiamos **1 priede 5 lentelėje**):

$$p(x) = \begin{cases} 0, & \text{kai } x \le 0, \\ -0.00478x + 0.03364, & \text{kai } 0 < x < 1, \\ 0, & \text{kai } x \ge 1. \end{cases}$$

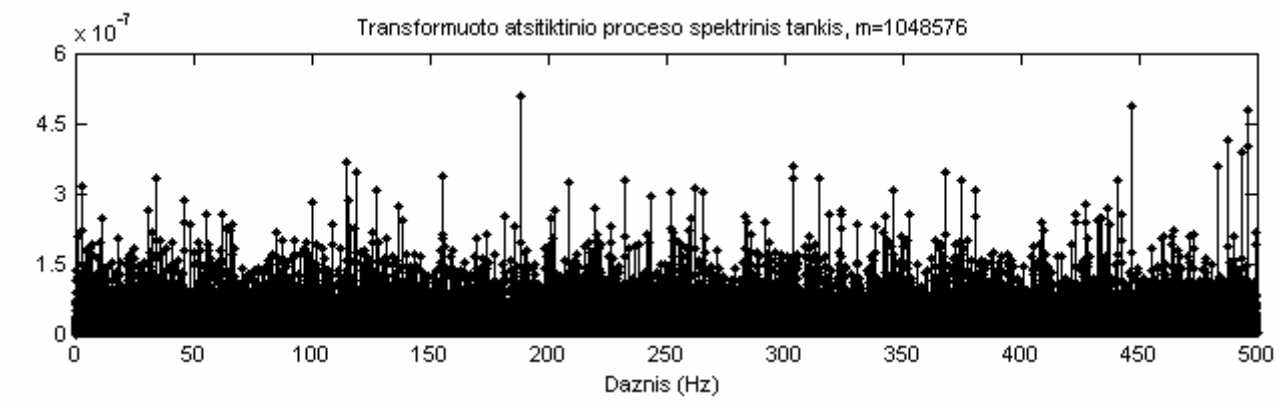
Randama pasiskirstymo funkcija:

$$F(x)=\begin{cases}0, & \text{kai } x \le 0,\\ \dfrac{-\dfrac{0.00478}{2}x^2+0.03364x}{-\dfrac{0.00478}{2}+0.03364}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x \ge 1.\end{cases}$$

AS transformuojami, statant juos į analizinę funkcijos išraišką. Skaičiuojama ir braižoma autokoreliacijos funkcija ir spektrinis tankis kombinacijai v1 (**2.22-2.23 pav.**). Visų kombinacijų autokoreliacijos funkcijos ir spektriniai tankiai pateikiami **1 priede 6-7 lentelėse**.

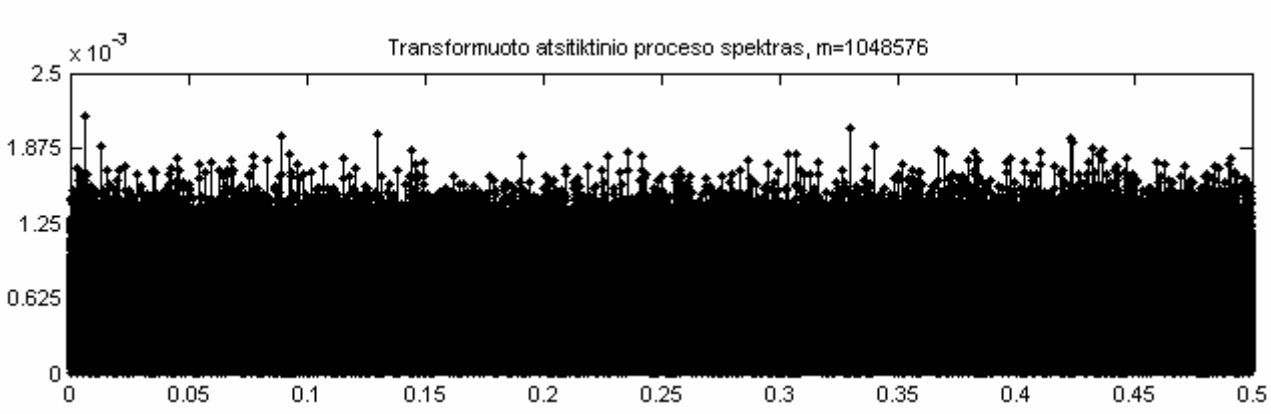


2.22 pav. Transformuoto atsitiktinio proceso (v1) autokoreliacijos funkcijos grafikas



2.23 pav. Transformuoto atsitiktinio proceso (v1) spektrinis tankis

Skaičiuojamas transformuoto atsitiktinio proceso spektras. Braižomas jo grafikas (**2.24 pav.**). Visų kombinacijų spektrų grafikai pateikiami **1 priede 8 lentelėje**.



2.24 pav. Transformuoto atsitiktinio proceso spektras

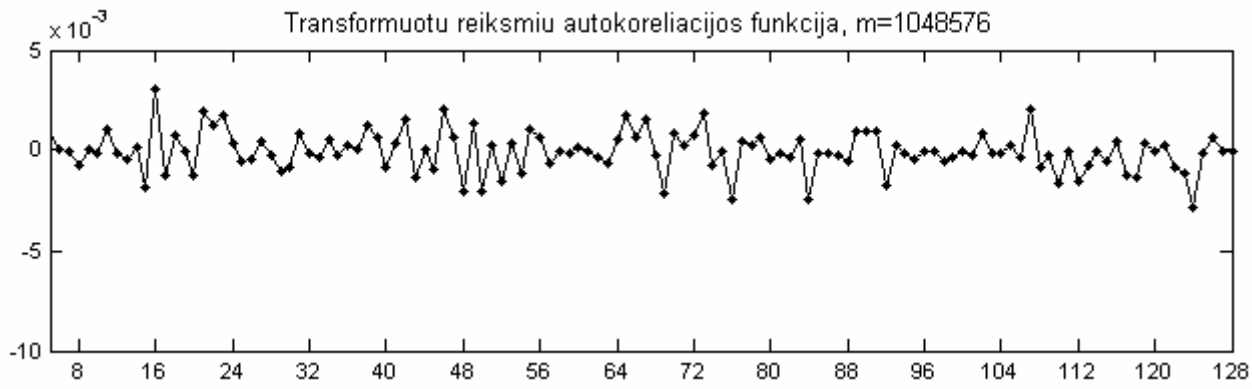
Histograma aproksimuojama parabole. Mažiausių kvadratų metodu kombinacijai v1 gaunama tokia tankio funkcijos išraiška (visos transformacijom reikalingos funkcijų išraiškos pateikiamos **1 priede 9 lentelėje**):

$$p(x)=\begin{cases}0, & \text{kai } x\le 0,\\ 0.00247x^2-0.00724x+0.03405, & \text{kai } 0<x<1,\\ 0, & \text{kai } x\ge 1.\end{cases}$$

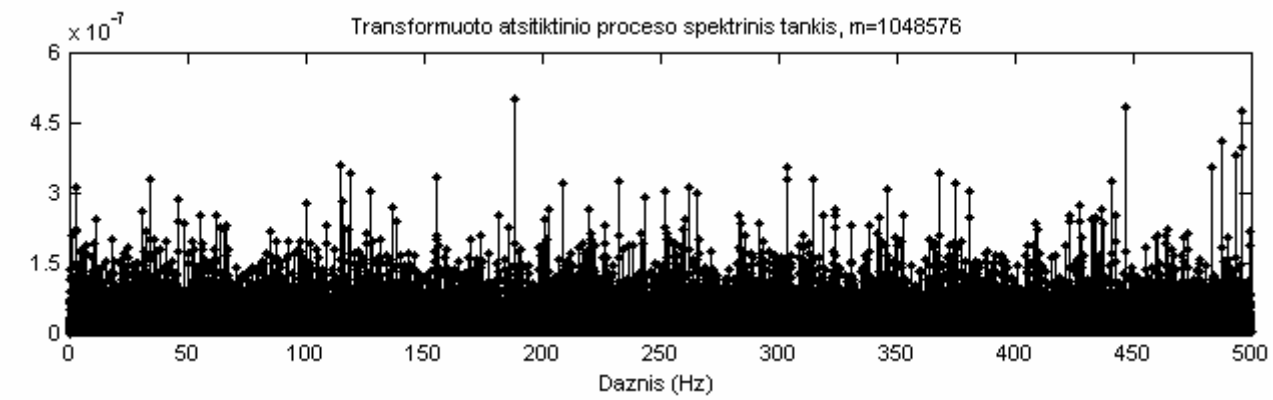
Randama pasiskirstymo funkcija:

$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00247}{3}x^3-\frac{0.00724}{2}x^2+0.03405x}{\frac{0.00247}{3}-\frac{0.00724}{2}+0.03405}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$$

AS transformuojami, statant juos į analizinę funkcijos išraišką. Skaičiuojama ir braižoma autokoreliacijos funkcija ir spektrinis tankis kombinacijai v1 (**2.25-2.26 pav.**). Visų kombinacijų autokoreliacijos funkcijos ir spektriniai tankiai pateikiami **1 priede 10-11 lentelėse**.

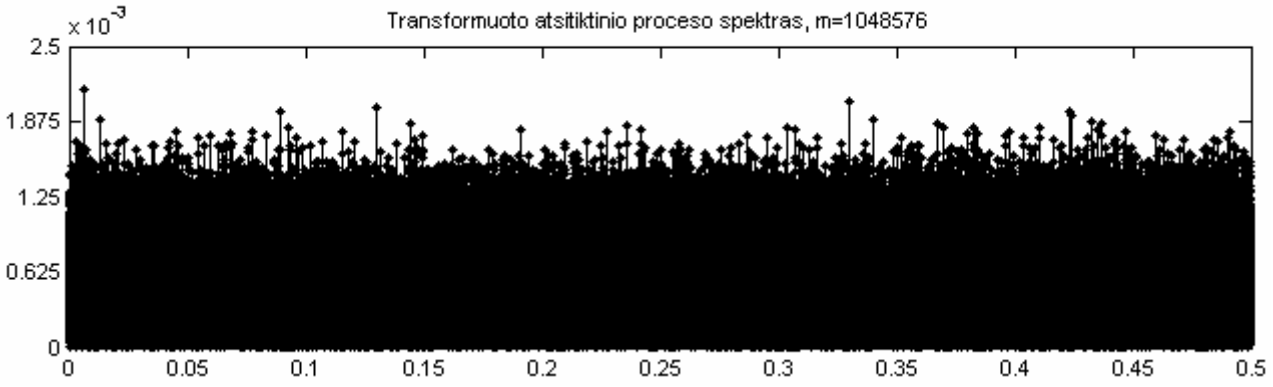


2.25 pav. Transformuoto atsitiktinio proceso (v1) autokoreliacijos funkcijos grafikas



2.26 pav. Transformuoto atsitiktinio proceso (v1) spektrinis tankis

Skaičiuojamas transformuoto atsitiktinio proceso spektras. Braižomas jo grafikas (**2.27 pav.**). Visų kombinacijų spektrų grafikai pateikiami **1 priede 12 lentelėje**.



2.27 pav. Transformuoto atsitiktinio proceso (v1) spektras

Tikrinamos abiem būdais transformuotų atsitiktinių procesų autokoreliacijos funkcijų lygybės nuliui. **2.9 lentelėje** pateikiamos vidutinės statistikos reikšmės kiekvienai kombinacijai ir sprendimai (H_0 atmetama arba neatmetama).

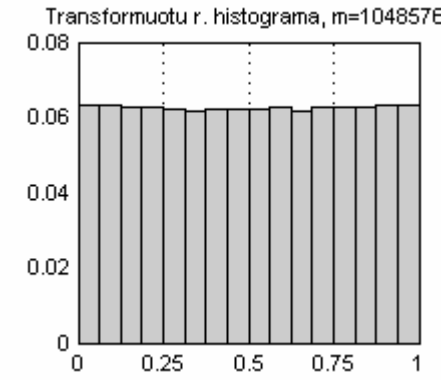
2.9 lentelė

Vidutinės Bokso Ljungo statistikos reikšmės

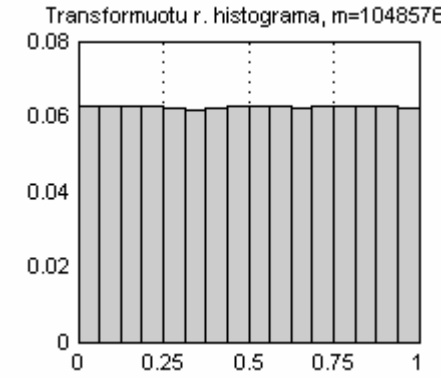
Kombinacija	Transformacija - Tiesė		Transformacija - Parabolė	
	Statistikos reikšmė	Sprendimas	Statistikos reikšmė	Sprendimas
v1	$1050590 < 1051000$	H_0 neatmetama	$1049920 < 1051000$	H_0 neatmetama
v2	$1053090 > 1051000$	H_0 atmetama	$1053220 > 1051000$	H_0 atmetama
v3	$1115660 > 1051000$	H_0 atmetama	$1113030 > 1051000$	H_0 atmetama
v4	$1075920 > 1051000$	H_0 atmetama	$1076010 > 1051000$	H_0 atmetama
v5	$1050680 < 1051000$	H_0 neatmetama	$1051120 > 1051000$	H_0 atmetama
v6	$1050510 < 1051000$	H_0 neatmetama	$1050470 < 1051000$	H_0 neatmetama

v7	$1076780 > 1051000$	H_0 atmetama	$1077900 > 1051000$	H_0 atmetama
v8	$1113350 > 1051000$	H_0 atmetama	$1114140 > 1051000$	H_0 atmetama

Skaičiuojamos ir braižomos kombinacijos v1 transformuotų atsitiktinių dydžių santykinių dažnių histogramos (**2.28-2.29 pav.**). Visų kombinacijų histogramos pateikiamos **1 priede 13 lentelėje**.



2.24 pav. Kombinacijos v1 santykinių dažnių histograma (transformuota tiese)



2.25 pav. Kombinacijos v1 santykinių dažnių histograma (transformuota parabole)

Pirsono χ^2 suderinamumo kriterijumi tikrinama ar transformuoti atsitiktiniai dydžiai yra pasiskirstę pagal tolygųjį skirstinį. **2.10 lentelėje** palyginimui pateikiamos vidutinės statistikos reikšmės ir sprendimai (H_0 atmetama arba neatmetama). Kritinė reikšmė - $\chi^2_{0.95}(15) = 25$ [1].

2.10 lentelė

Vidutinės Pirsono χ^2 statistikos reikšmės

Kombinacija	Transformacija - Tiesė		Transformacija - Parabolė	
	Statistikos reikšmė	Sprendimas	Statistikos reikšmė	Sprendimas
v1	58.74	H_0 atmetama	16.21	H_0 neatmetama
v2	58.20	H_0 atmetama	14.12	H_0 neatmetama
v3	205.04	H_0 atmetama	16.85	H_0 neatmetama

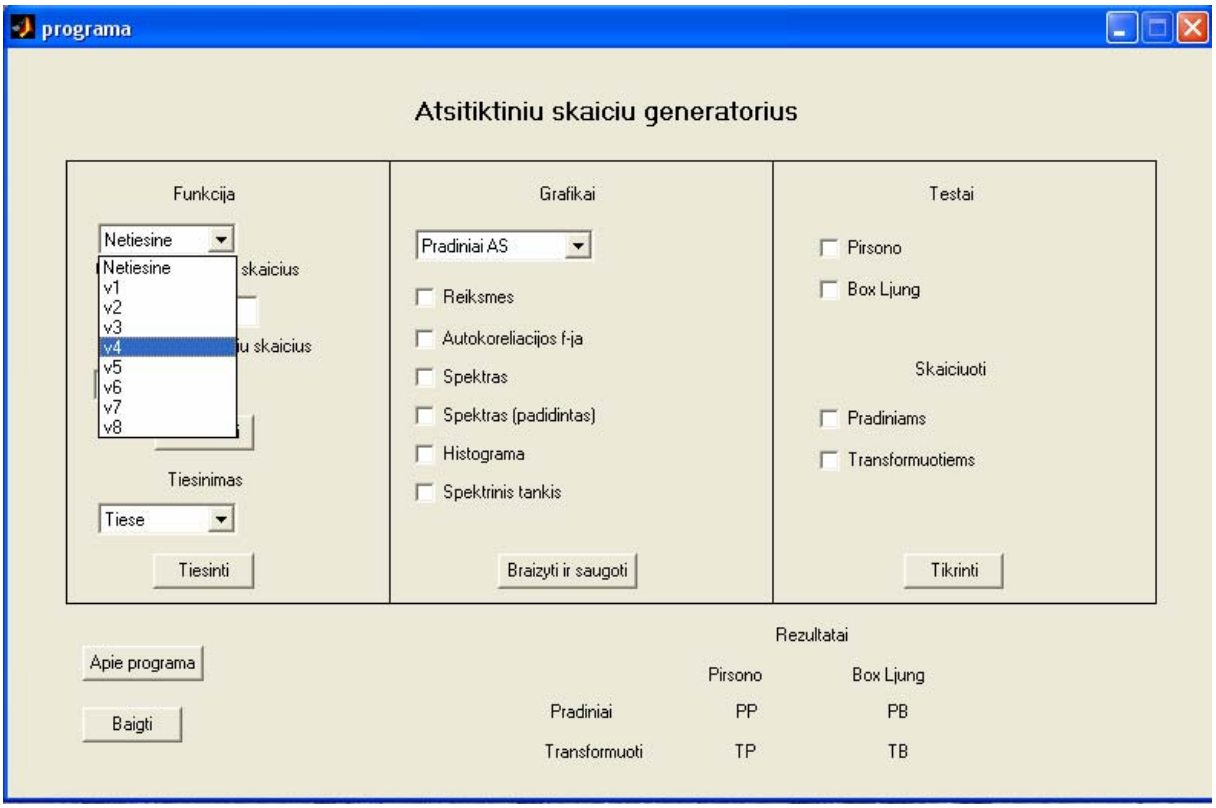
v4	112.21	H_0 atmetama	24.37	H_0 neatmetama
v5	58.80	H_0 atmetama	13.48	H_0 neatmetama
v6	56.77	H_0 atmetama	15.39	H_0 neatmetama
v7	101.09	H_0 atmetama	12.09	H_0 neatmetama
v8	165.88	H_0 atmetama	21.83	H_0 neatmetama

3. PROGRAMINĖ REALIZACIJA IR INSTRUKCIJA VARTOTOJUI

Nagrinėjamų atsitiktinių skaičių generatorių tyrimas atliktas matematiniu paketu MATLAB. Sukurta grafinė vartotojo sąsaja susidedanti iš keturių pagrindinių dalių:

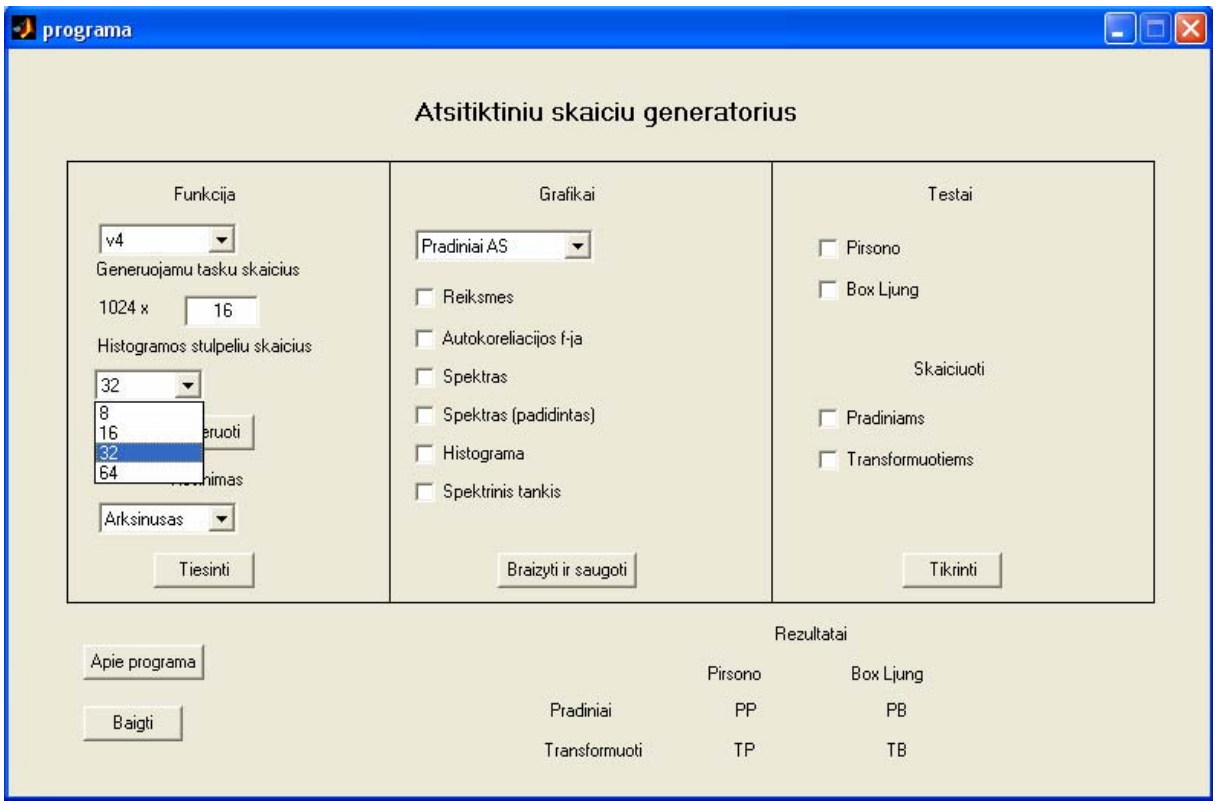
- atsitiktinių skaičių (AS) generavimas ir transformavimas,
- grafikų braižymas ir saugojimas,
- statistinių hipotezių tikrinimas,
- rezultatų pateikimas ir informacija vartotojui.

Pirmojoje dalyje iš sąrašo pasirenkamas AS generavimo algoritmas (**3.1 pav.**).



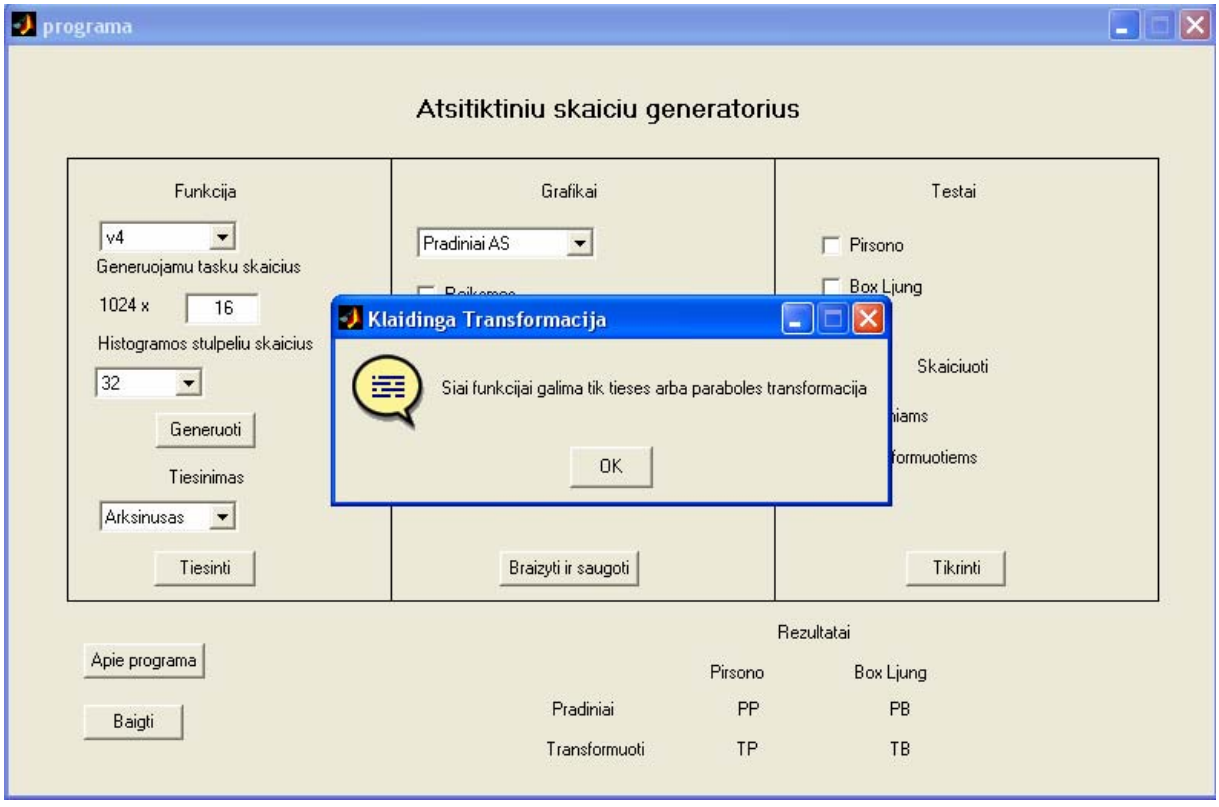
3.1 pav. Atsitiktinių skaičių generavimo algoritmo pasirinkimas

Vartotojas gali nurodyti generuojamų taškų skaičių, taip pat pasirinkti kiek stulpelių turėtų turėti histograma (**3.2 pav.**). Įvedamas generuojamų taškų skaičius turėtų būti sveikas skaičius. Jei bus įvestas realus skaičius arba simbolis, programa išveda pranešimą apie klaidą ir reikia iš naujo įvedinėti generuojam taškų skaičių. AS generavimas pagal pasirinktus parametrus vyksta paspaudus mygtuką „Generuoti“. Šio mygtuko paspaudimu taip pat vykdomas ir autokoreliacijos funkcijos, spektro, spektrinio tankio bei histogramos skaičiavimai. Vykstant skaičiavimams, vartotojui rodoma įvykių juostelė (angl. *progress bar*) informuojanti kiek dar liko iki skaičiavimų pabaigos.



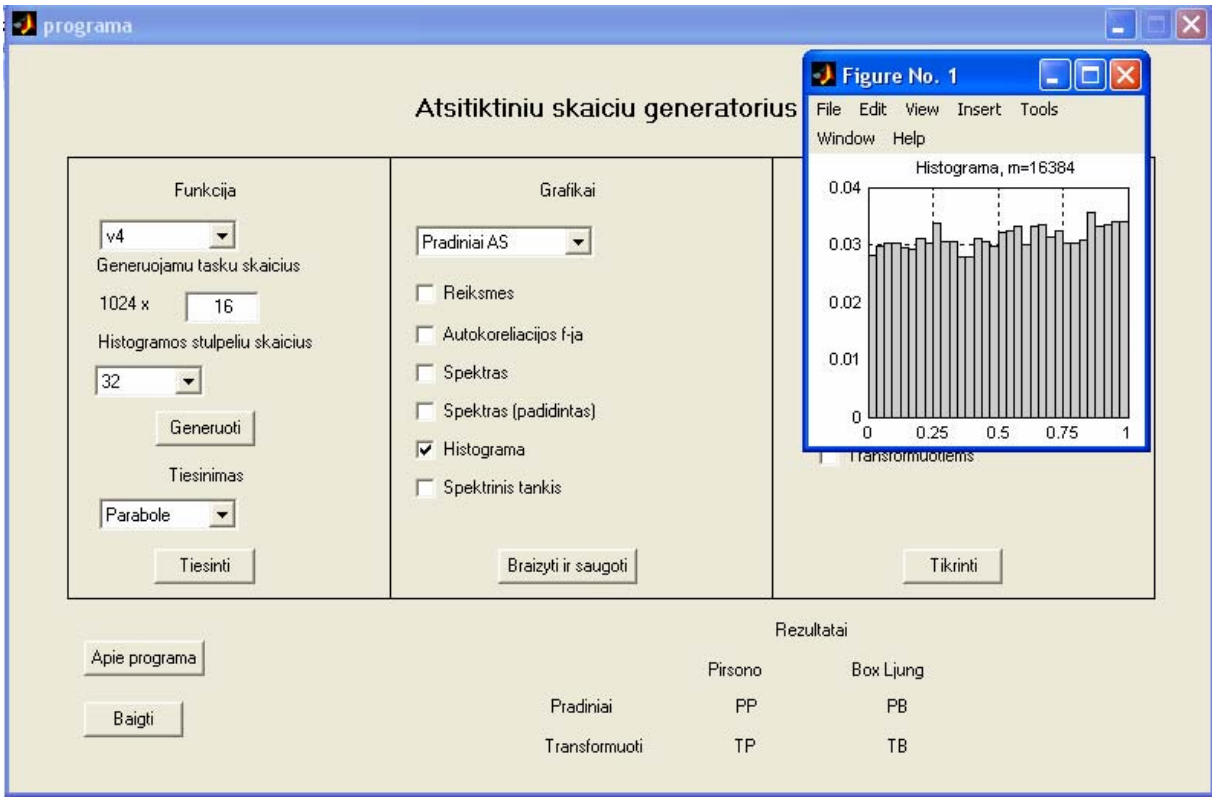
3.2 pav. Generuojamų taškų ir histogramos stulpelių skaičiaus pasirinkimas

Sugeneravus AS galima pasirinkti norimą transformacijos funkciją ir juos transformuoti. Kiekvienas generavimo algoritmas turi dvi galimas transformacijas. Pasirinkęs netinkamą – vartotojas bus perspėtas pranešimu, kad atitinkama transformacija negalima (**3.3 pav.**).



3.3 pav. Transformacijos funkcijos pasirinkimas

Antrojoje dalyje vartotojas gali pasirinkti kokius grafikus norėtų braižyti ir saugoti (**3.4 pav.**). Jei AS buvo sugeneruoti, bet nebuvo transformuoti, norint braižyti transformuotų AS grafikus, vartotojas bus perspėjamas, kad AS reikia transformuoti.



3.4 pav. Pasirinktų grafikų braižymas ir saugojimas

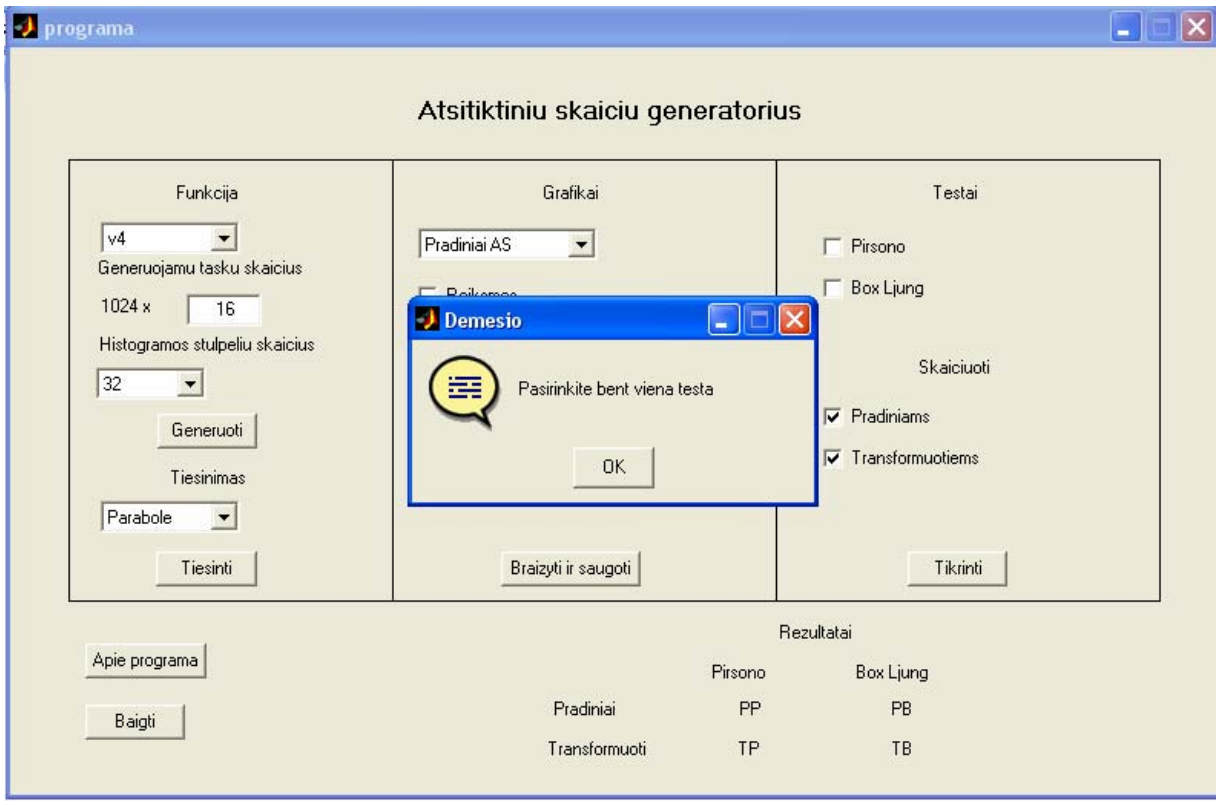
Trečiojoje dalyje vartotojas gali pasirinkti kokias nulines hipotezes norėtų patikrinti:

- Pirsosno – AS yra pasiskirstę pagal tolygųjį skirstinį,
- Box Ljung – AS yra nekoreliuoti.

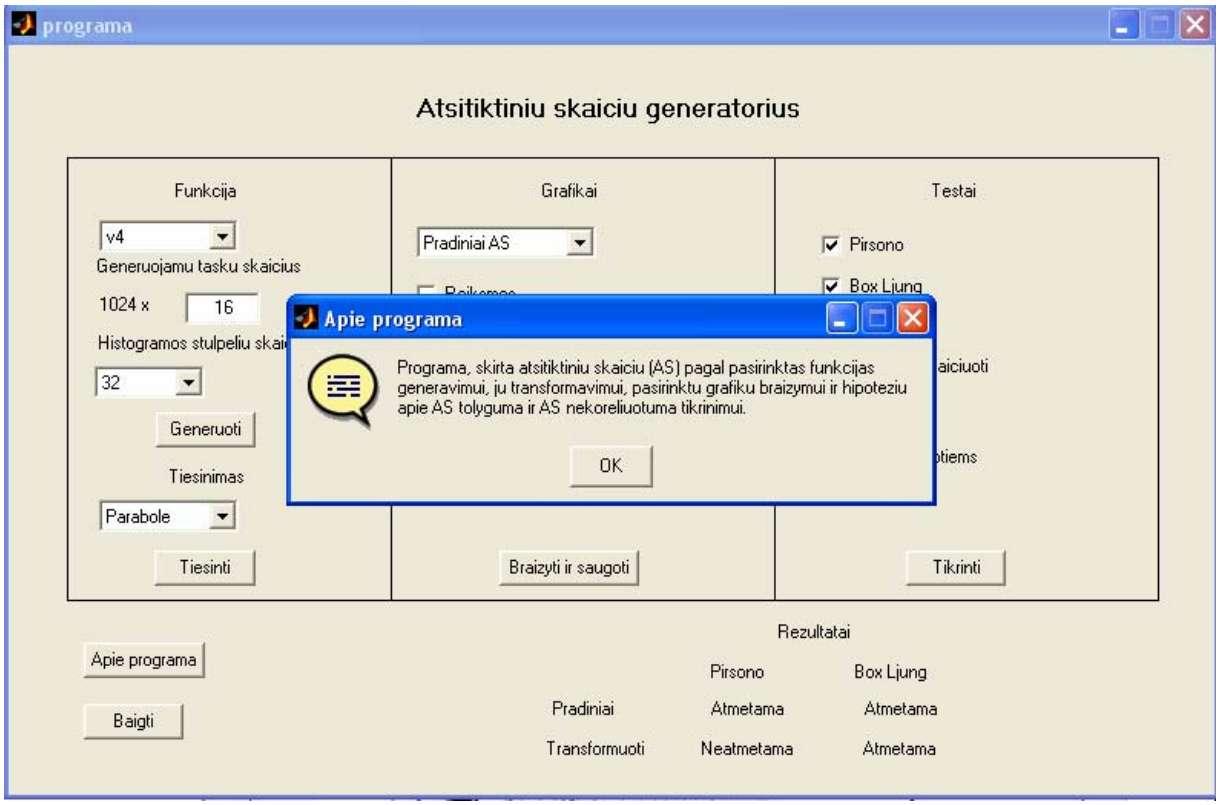
Galima pasirinkti, kad būtų skaičiuojamas kuris nors vienas iš šių testų arba abu. Taip pat galima pasirinkti kokiems AS bus skaičiuojama: pradiniams ar transformuotiems. Nepasirinkus nei vieno testo, vartotojui pranešama apie klaidą ir norodoma kad reikia pasirinkti bent vieną testą (**3.5 pav.**). Pasirinkus kad testai būtų skaičiuojami transformuotiems AS, kai transformacija nebuvo atlikta, pranešama, kad AS pirmiau reikia transformuoti. Rezultatai pateikiami ketvirtojoje dalyje ir gali būti tokie:

- atmetama – atitinkama nulinė hipotezė atmetama,
- neatmetama – atitinkama nulinė hipotezė neatmetama.

Tai pat šioje dalyje yra informacijos apie programą ir pabaigos mygtukai (**3.6 pav.**).



3.5 pav. Pranešimas apie klaidą, nepasirinkus nei vieno testo



3.6 pav. Informacija apie programą

DISKUSIJA

Šiame darbe buvo tiriamas netiesinis kongriuentinis generatorius ir aštuonios tiesinio ir netiesinio kongriuentinių generatorių kombinacijos. Tiesinis kongriuentinis generatorius pasirinktas kaip etaloninis, su kuriuo yra lyginami gautieji rezultatai. Buvo skaičiuojamos tokios charakteristikos:

- autokoreliacijos funkcija,
- spektras,
- spektrinis tankis,
- histograma.

Taip pat buvo tikrinamos hipotezės apie atsitiktinių skaičių pasiskirstymą pagal tolygųjį skirstinį ir nekoreliuotumą.

Autokoreliacijos funkcija buvo skaičiuojam pradiniams ir transformuotiems atsitiktiniams procesams. Buvo pastebėta, kad didėjant generuojamų taškų skaičiui autokoreliacijos funkcija tampa artima nuliui. Tam, kad tai patikrinti buvo skaičiuojama Bokso Ljungo statistika. Buvo pastebėta, kad:

- AS gauti iš netiesinio kongriuentinio generatoriaus yra geresni nei gauti iš kombinacijų v1-v8 koreliuotumo prasme, t.y. vidutiniškai jie buvo nekoreliuoti (testas atliktas dvidešimčiai skirtingų AS realizacijų, gautos kritinės Bokso Ljungo statistikos reikšmės ir paskaičiuotas jų vidurkis), bet blogesni nei gauti iš tiesinio kongriuentinio generatoriaus (**4.1 lentelė**). Iš kombinacijų v1-v8 vidutiniškai nekoreliuotus AS generavo tik v1, v5 ir v6. Paskaičiuotų vidutinių statistikų reikšmės nuo kritinės reikšmės (1051000) skiriasi nuo -1% iki $+3.6\%$, o tai reiškia, kad tik nuo konkrečios realizacijos priklausys ar hipotezė apie koreliuotumą bus atmetama ar ne.

1 lentelė

Vidutinių Bokso Ljungo statistikos reikšmių palyginimas

Generatorius	*Vidutinė statistikos reikšmė*	*Sprendimas*
Tiesinis kongiuentinis	1048220	H_0 neatmetama
Netiesinis kongriuentinis	1049515	H_0 neatmetama
Kominacija v1	1049940	H_0 neatmetama
Kominacija v2	1051875	H_0 atmetama
Kominacija v3	1089525	H_0 atmetama
Kominacija v4	1067490	H_0 atmetama
Kominacija v5	1049560	H_0 neatmetama
Kominacija v6	1050295	H_0 neatmetama
Kominacija v7	1068735	H_0 atmetama
Kominacija v8	1089010	H_0 atmetama

- Netiesiniam kongriuentiniam generatoriui ir kombinacijom v1-v8 buvo parinktos transformacijų funkcijos. I – oji transformacija netiesiniam generatoriui – arksinusas, kombinacijom v1-v8 – tiesė. II – oji transformacija visais atvejais yra parabolė. Tiesinio kongriuentinio generatoriaus generuojamiems AS transformacija neatliekama, nes jie jau yra pasiskirstę pagal tolygųjį skirstinį. Stebimos panašios tendencijos, kaip ir pradinių AS atveju: netiesinio generatoriaus generuojami AS yra vidutiniškai nekoreliuoti. Iš kombinacijų v1-v8 vidutiniškai nekoreliuotus AS generavo tik v1, v5 ir v6 (**4.2 lentelė**). Šiuo atveju skirtumas yra truputi didesnis – iki $+5.9\%$. Nustatyta, kad koreliuotumo prasme po tiesinio generatoriaus geriausias yra netiesinis generatorius.

2 lentelė

Vidutinių Bokso Ljungo statistikos reikšmių palyginimas transformuotiems AS

Generatorius	I – oji transformacija		II – oji transformacija	
	Statistikos reikšmė	Sprendimas	Statistikos reikšmė	Sprendimas
Netiesinis	1049490	H_0 neatmetama	1050070	H_0 neatmetama
v1	1050590	H_0 neatmetama	1049920	H_0 neatmetama
v2	1053090	H_0 atmetama	1053220	H_0 atmetama
v3	1115660	H_0 atmetama	1113030	H_0 atmetama
v4	1075920	H_0 atmetama	1076010	H_0 atmetama
v5	1050680	H_0 neatmetama	1051120	H_0 atmetama
v6	1050510	H_0 neatmetama	1050470	H_0 neatmetama
v7	1076780	H_0 atmetama	1077900	H_0 atmetama
v8	1113350	H_0 atmetama	1114140	H_0 atmetama

Nagrinėjant santykinių dažnių histogramas buvo pastebėta:

- AS gautų iš netiesinio kongriuentinio generatoriaus santykinių dažnių histograma buvo nepanaši nei į vieną iš likusių kombinacijų (**2.9 pav.** ir **1 PRIEDAS 4 lentelė**). Tarp kombinacijų v1-v8 pastebėtos tendencijos susijusios su AS generavimo algoritmo pasirinkimu (v1 ir v5 kombinacijos turi tas pačias netiesines, bet skirtingas tiesines dalis; analogiškai yra su v2 ir v6, v3 ir v7, bei v4 ir v8). Galima spręsti, kad tiesinės dalies pasikeitimas (nekintant netiesinei daliai) nedaug keičia generuojamų AS santykinių dažnių histogramą.
- Lyginant vidutines Pirsono χ^2 statistikos reikšmes buvo pastebėta, kad tiesinio kongriuentinio generatoriaus atveju AS visais atvejais buvo pasiskirstę pagal tolygųjį skirstinį. Netiesinio generatoriaus ir kombinacijų v1-v8 atveju buvo gauta, kad pradiniai AS nėra pasiskirstę pagal tolygųjį skirstinį (**4.3 lentelė**).

3 lentelė

Vidutinių Pirsono χ^2 statistikos reikšmių palyginimas

Generatorius	Vidutinė statistikos reikšmė	Sprendimas
Tiesinis	13.9748	H_0 neatmetama
Netiesinis	393552	H_0 atmetama
v1	2083	H_0 atmetama
v2	2881	H_0 atmetama
v3	4351	H_0 atmetama
v4	1570	H_0 atmetama
v5	2908	H_0 atmetama
v6	2086	H_0 atmetama
v7	1584	H_0 atmetama
v8	4215	H_0 atmetama

- Nagrinėjant transformuotų AS santykinių dažnių histogramas nustatomos geriausios transformacijų išraiškos. Jos nustatomos mažiausių kvadratų metodu. Geriausiomis laikomos tos, kuriomis transformuoti AS yra pasiskirstę pagal tolygųjį skirstinį. Pasirenkant tranformacijos pavidalą buvo bandyta taikyti ir kubinę parabolę. Determinacijos koeficiento R^2 prasme ji tiko geriausiai, bet buvo priimta hipotezė apie koeficiento prie aukščiausios eilės nario lygybę nuliui, todėl šios transformacijos buvo atsisakyta. Nustatyta, kad geriausia transformacija netiesiniam kongriuentiniam generatoriui yra arksinusas, o kombinacijom v1-v8 – parabolė (**4.4 lentelė**).

4 lentelė

Vidutinių Pirsono χ^2 statistikos reikšmių palyginimas transformuotiems AS

Generatorius	I – oji transformacija		II – oji transformacija	
	Statistikos reikšmė	Sprendimas	Statistikos reikšmė	Sprendimas
Netiesinis	14,0	H_0 neatmetama	150126	H_0 atmetama
v1	58.74	H_0 atmetama	16.21	H_0 neatmetama
v2	58.20	H_0 atmetama	14.12	H_0 neatmetama
v3	205.04	H_0 atmetama	16.85	H_0 neatmetama
v4	112.21	H_0 atmetama	24.37	H_0 neatmetama
v5	58.80	H_0 atmetama	13.48	H_0 neatmetama
v6	56.77	H_0 atmetama	15.39	H_0 neatmetama
v7	101.09	H_0 atmetama	12.09	H_0 neatmetama
v8	165.88	H_0 atmetama	21.83	H_0 neatmetama

Lyginant tiesinį ir netiesinį kongriuentinius generatorius, bei kombinacijas v1-v8 nustatyta, kad nagrinėti generatoriai savo kokybe dauguma atvejų yra blogesni už tiesinį. Juo generuojami AS yra pasiskirstę tolygiai, bei yra nekoreliuoti. Šio generatoriaus pagrindinis trūkumas – jo tiesiškumas, jis nėra tinkamas kriptografijai, nes yra per daug nuspėjamas, todėl ieškomas tarp kitų nagrinėtų generatorių toks, kuris būtų ne toks nuspėjamas, bei turėtų panašias kokybines savybes. Lyginant transformuotų AS vidutines Pirsono χ^2 statistikos reikšmes su tiesinio generatoriaus vidutine atitinkamos statistikos reikšme pastebėta, kad v7 ir v5 parabolės transformacijos atveju jos yra mažesnės nei tiesinio, o netiesinio – arksinuso transformacijos atveju – labai artima tiesiniam. Kombinacijų v5 ir v7 atveju gauta, kad hipotezės ape autokoreliacijos funkcijos lygybę nuliui atmetamos. Apibendrinant šias dvi savybes nustatoma, kad geriausias iš likusių būtų netiesinis kongriuentinis generatorius

IŠVADOS

- Nustatyta, kad geriausias nagrinėtų savybių prasme būtų tiesinis kongriuentinis generatorius, tačiau jis netinkamas kriptografijai, nes yra per daug nuspėjamas. Iš likusių generatorių artimiausias tiesiniam buvo netiesinis kongriuentinis generatorius.

- Nustatyta, kad geriausia (Pirsono χ^2 statistikos prasme) transformacija generuotų AS skirstinį paverčianti tolygiu yra: netiesinio kongriuentinio generatoriaus atveju – arksinusas, o kitiem nagrinėjamiem generatoriam v1-v8 – parabolė.

- Nustatyta, kad nulinės hipotezės apie autokoreliacijos funkcijos lygybę nuliui atmetimas arba neatmetimas priklauso nuo:
  - pasirinkto AS generavimo algoritmo,
  - imties dydžio (generuojamų AS skaičiaus).

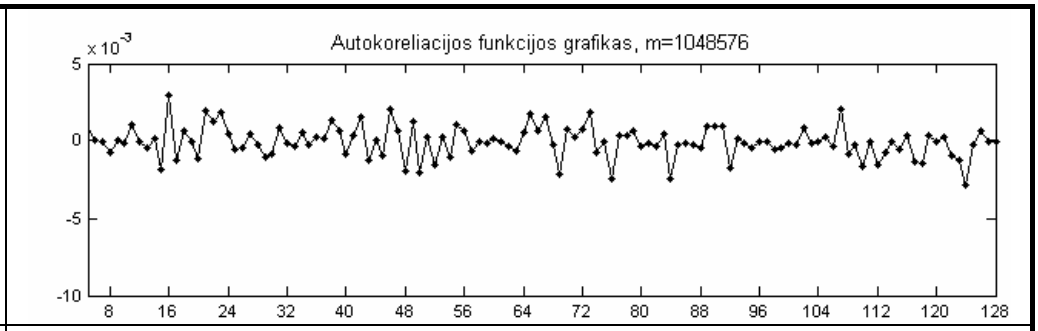
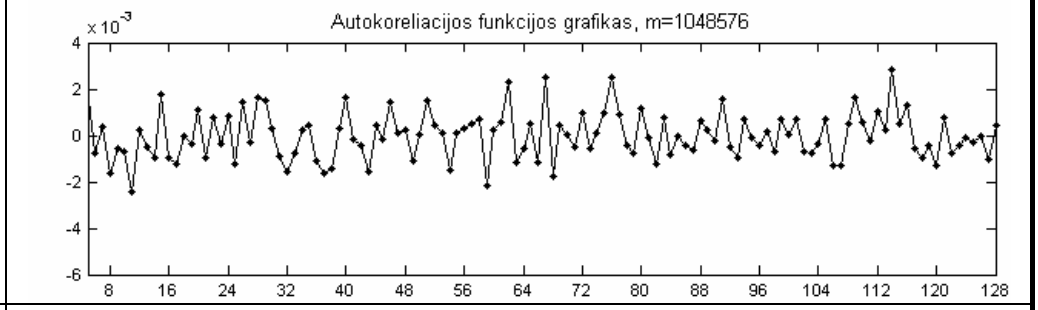
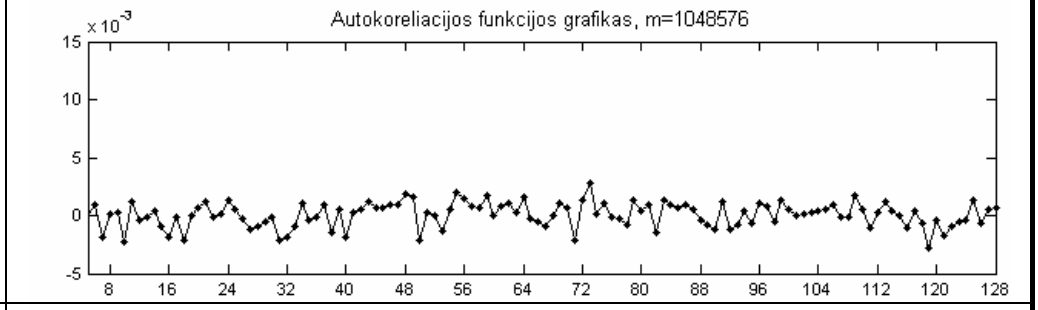
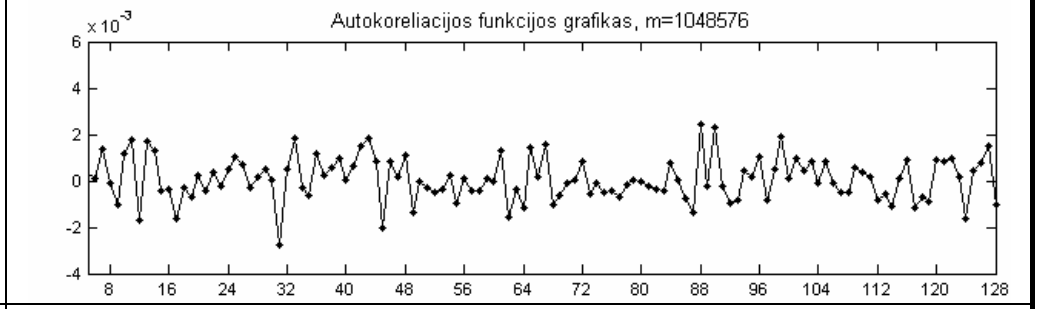
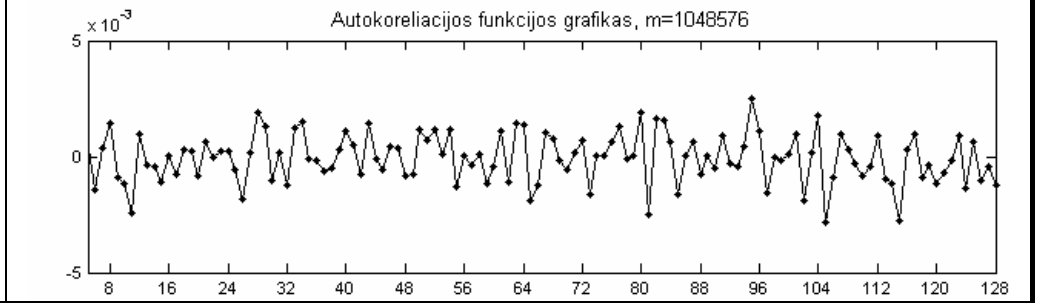
LITERATŪRA

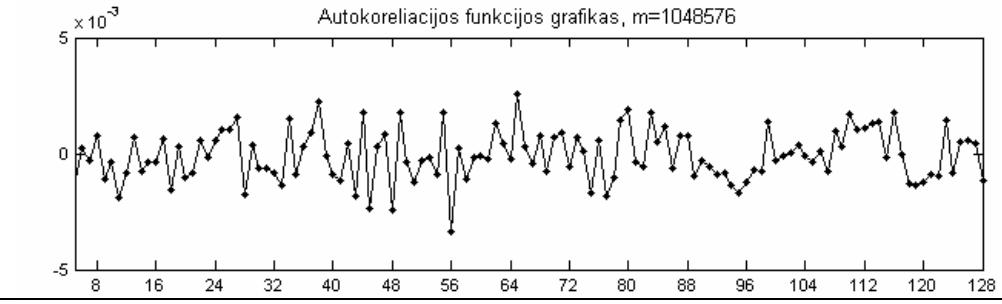
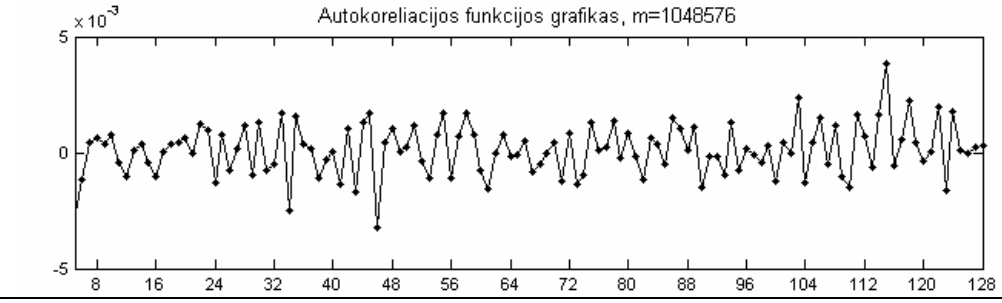
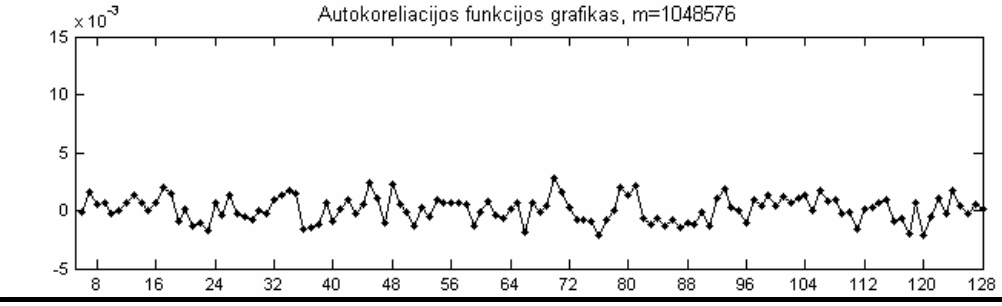
1. Aksomaitis A. Tikimybių teorija ir statistika, ISBN 9986-13-893-0, Kaunas, „Technologija“, 2002, p. 347.
2. Kligienė N. Įvadas į atsitiktinių sekų statistinę analizę, ISBN 9986-05-363-3, Vilnius, „Technika“, 1998, p. 140.
3. Kruopis J. Matematinė statistika, ISBN 5-420-01015-1, Vilnius, „Mokslo ir enciklopedijų leidykla“, 1993, p. 414.
4. Barila A., Barilienė L., Jakutavičius A., Karbauskas J., Palevičius R. Programavimo Matlab terpėje laboratoriniai darbai,ISBN 9955-09-339-0, Kaunas, „Technologija“, 2005, p. 135.
5. Knuth Donald E. The Art of Computer Programming, Vol.2, ISBN 0-201-03822-6, „Addison-Wesley Publishing Company“, 1981, p.704.
6. Ruey S. Tsay, Analysis of Financial Time Series. John Wiley & Sons, Inc. 2002. ISBN 0-471-41544-8.
7. C. W. J. Granger, M. W. Watson, Time Series and Spectral Methods in Econometrics, Elsevier Science Publishers BV, 1984.
8. http://en.wikipedia.org/wiki/Blum_Blum_Shub
9. http://www.fact-index.com/b/bl/blum_blum_shub.html
10. http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/ewhat-is-mt.html
11. http://www.agner.org/random/mother/
12. http://en.wikipedia.org/wiki/Discrete_fourier_transform
13. http://en.wikipedia.org/wiki/Spectral_density
14. http://katr.vtu.lt/leonidas/konspi/konspektas1_files/konspektas1.htm
15. http://random.mat.sbg.ac.at/generators/
16. http://www.mathcom.com/corpdir/techinfo.mdir/scifaq/q210.html
17. http://en.wikipedia.org/wiki/Linear_feedback_shift_register
18. http://en.wikipedia.org/wiki/Linear_congruential_generator
19. http://crypto.mat.sbg.ac.at/results/karl/server/node3.html
20. http://www.math.nyu.edu/~cai/Courses/Derivatives/compfin_lecture_1.pdf
21. http://en.wikipedia.org/wiki/Lagged_Fibonacci_generator
22. http://sprng.cs.fsu.edu/Version1.0/paper/node8.html

1 PRIEDAS. Grafikai

1 lentelė

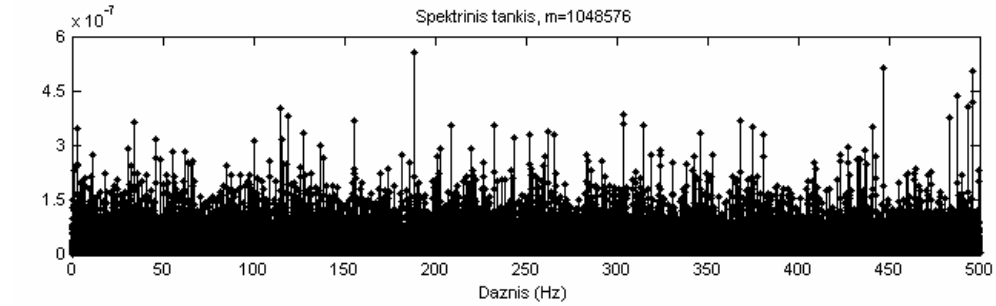
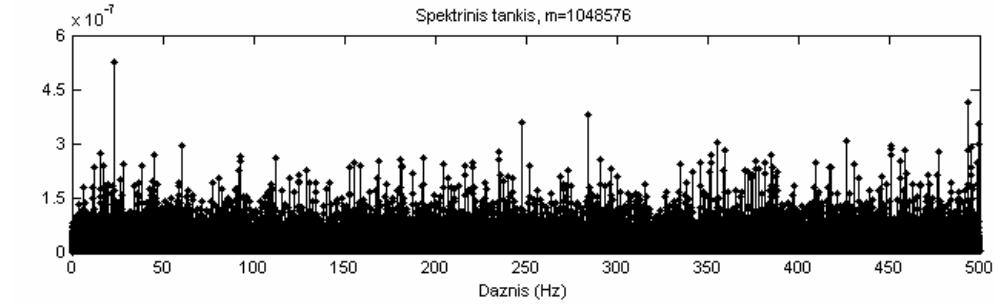
Autokoreliacijos funkcijos grafikai

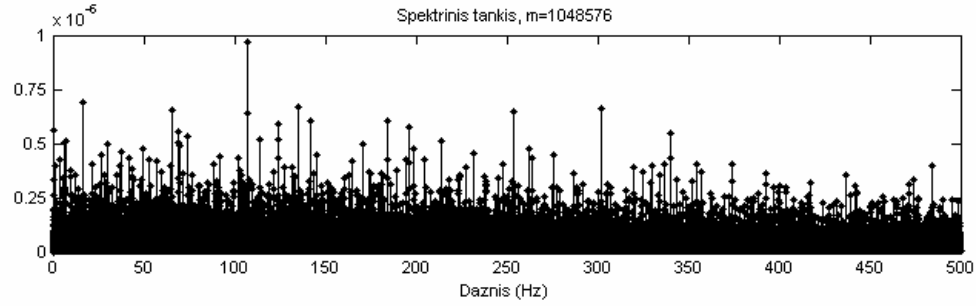
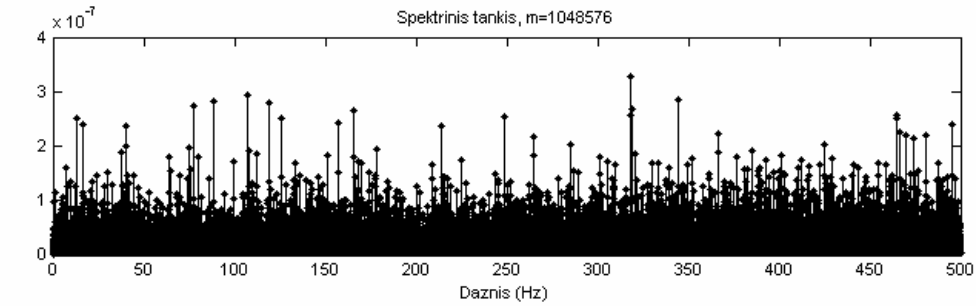
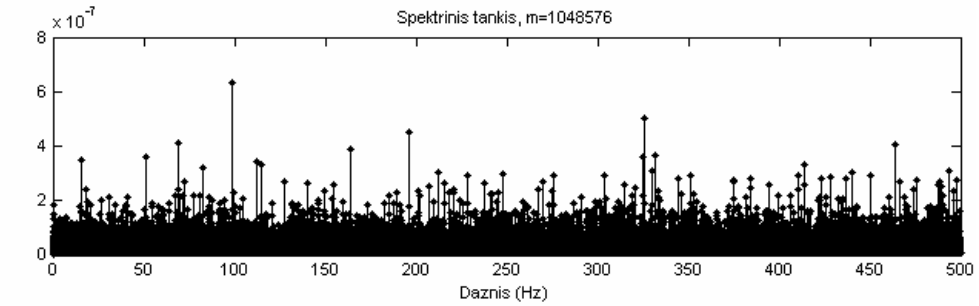
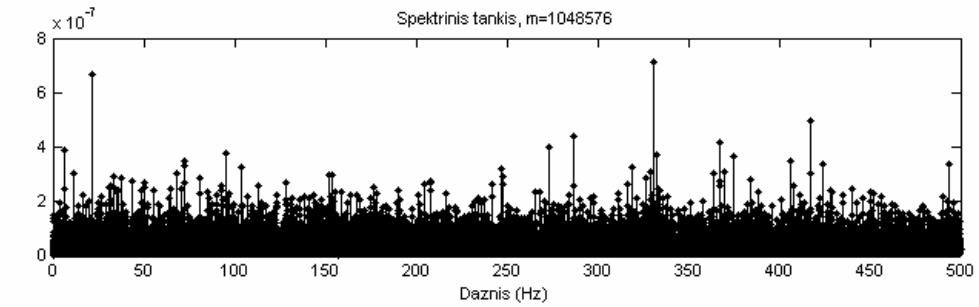
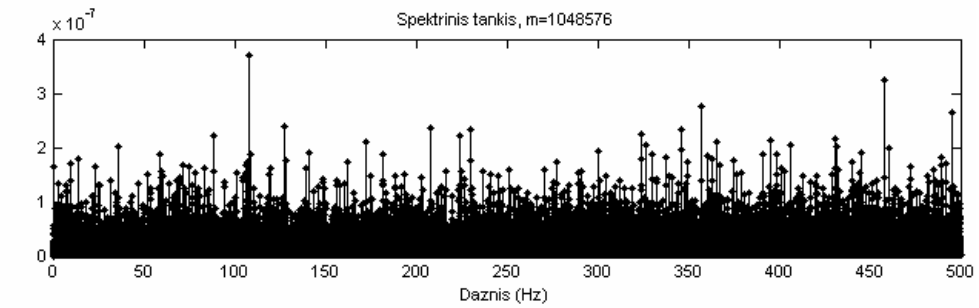
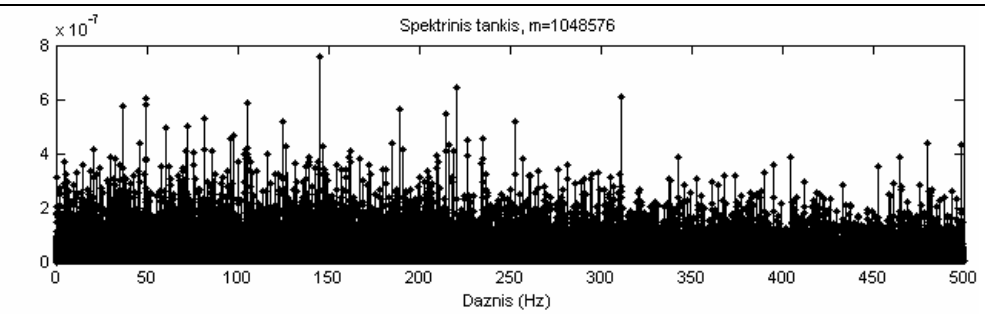
v1	
v2	
v3	
v4	
v5	

v6	
v7	
v8	

2 lentelė

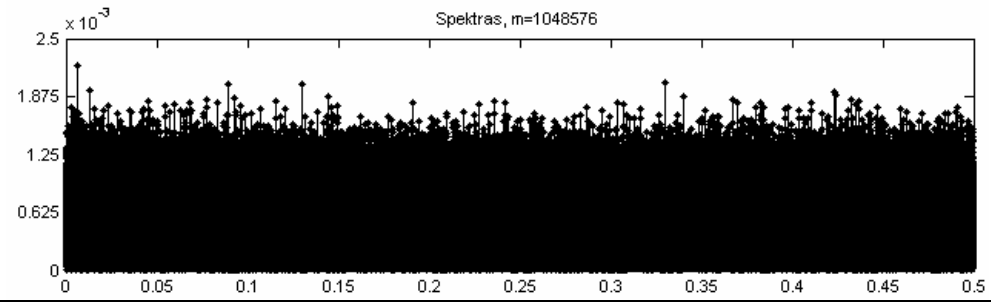
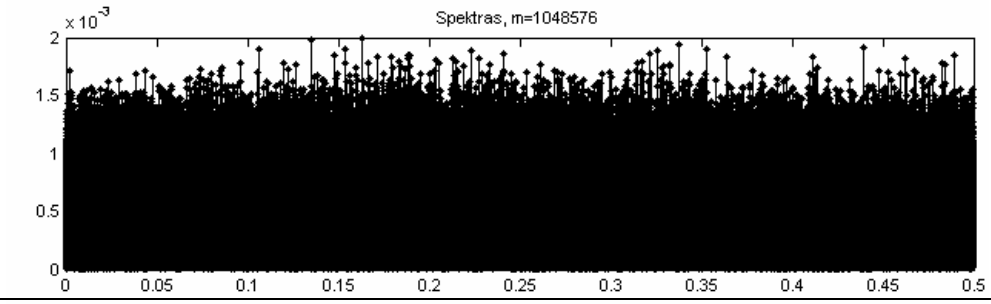
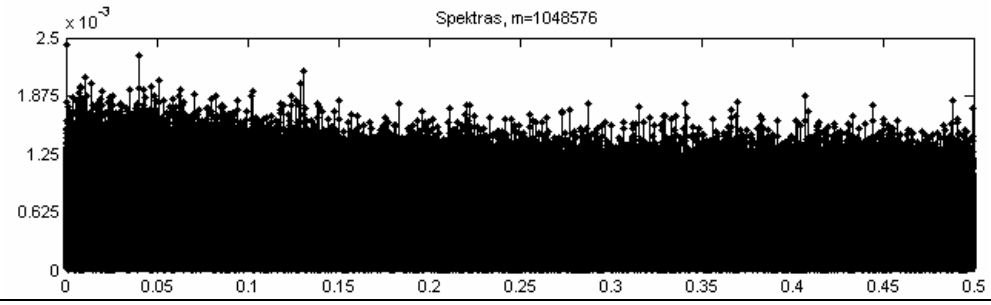
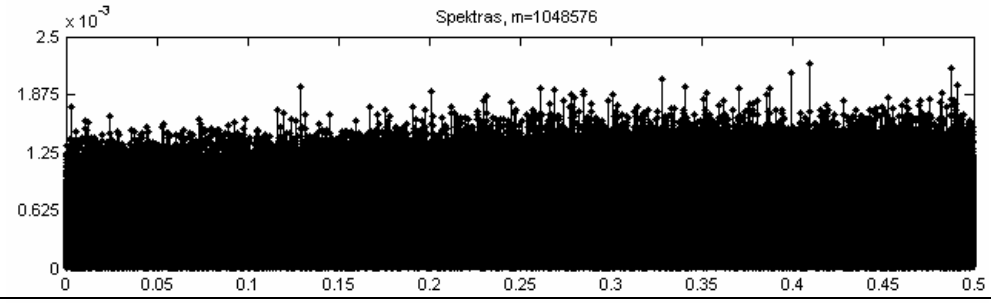
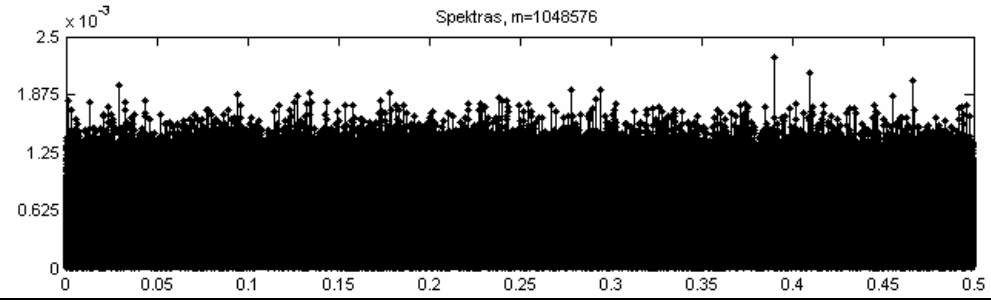
Spektrinio tankio grafikai

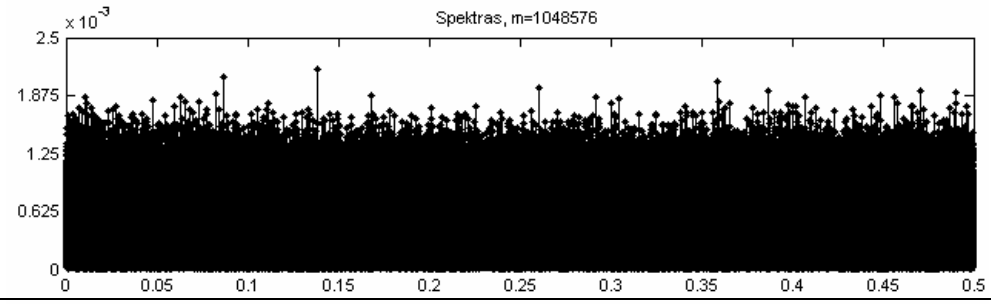
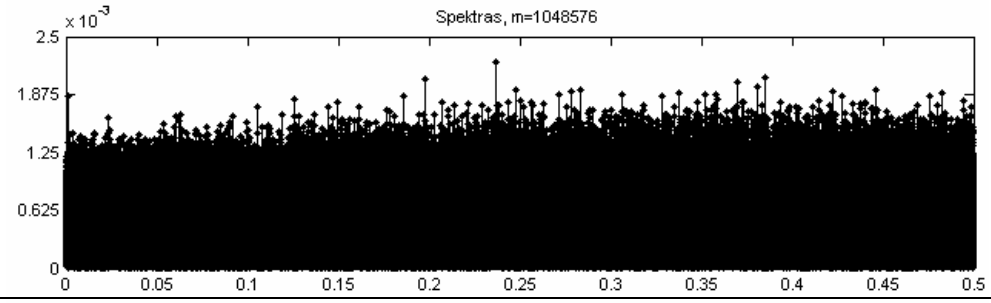
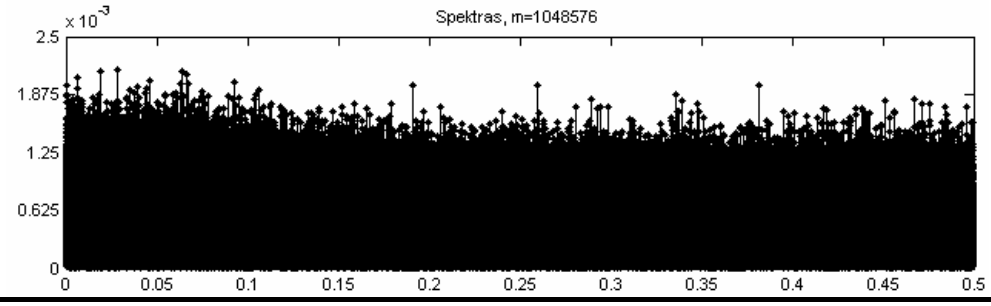
v1	
v2	

v3	
v4	
v5	
v6	
v7	
v8	

3 lentelė

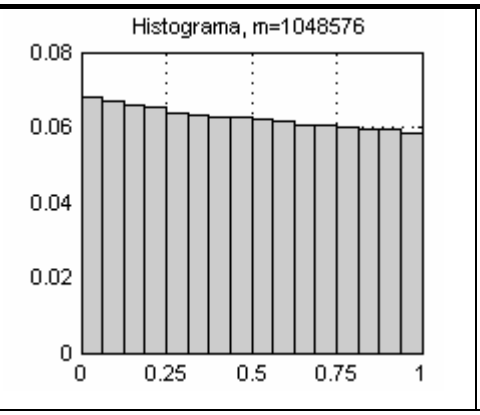
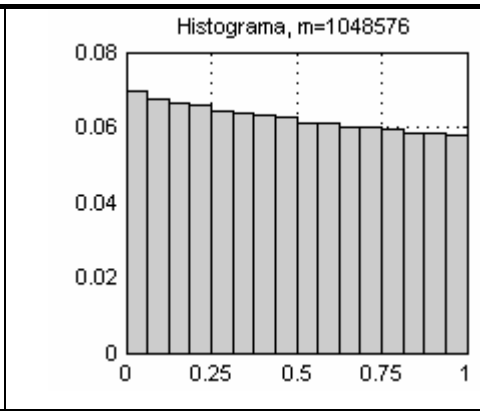
Spektro grafikai

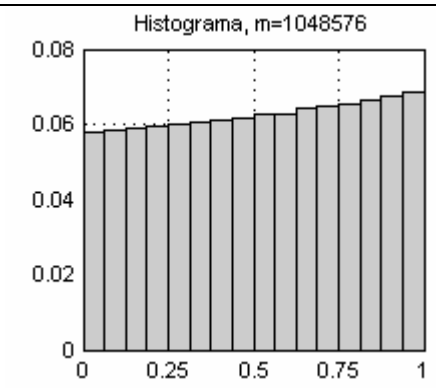
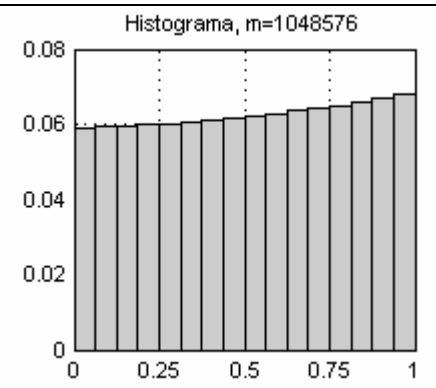
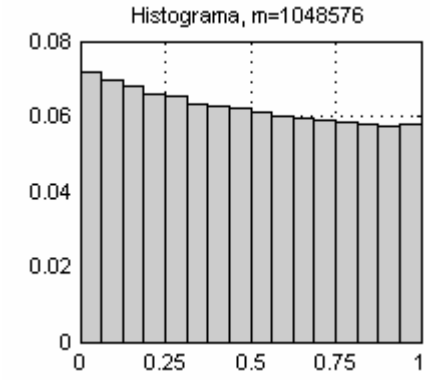
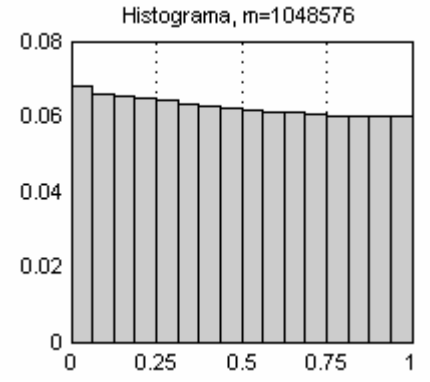
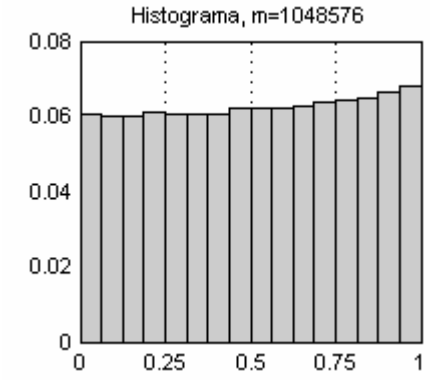
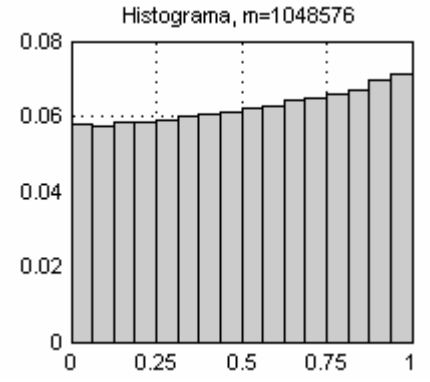
v1	
v2	
v3	
v4	
v5	

v6	
v7	
v8	

4 lentelė

Histogramos

v1		v5	

v2		v6	
v3		v7	
v4		v8	

5 lentelė

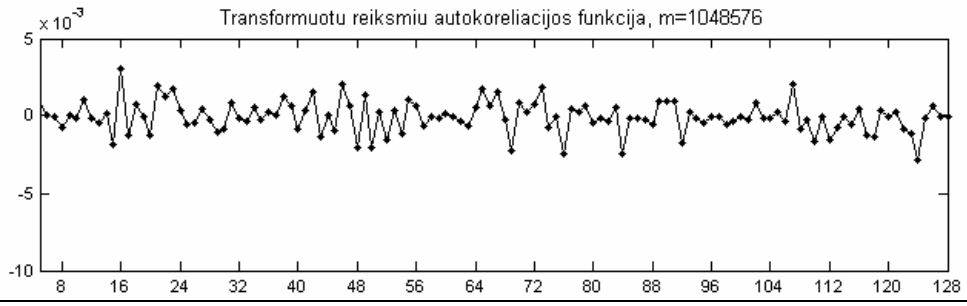
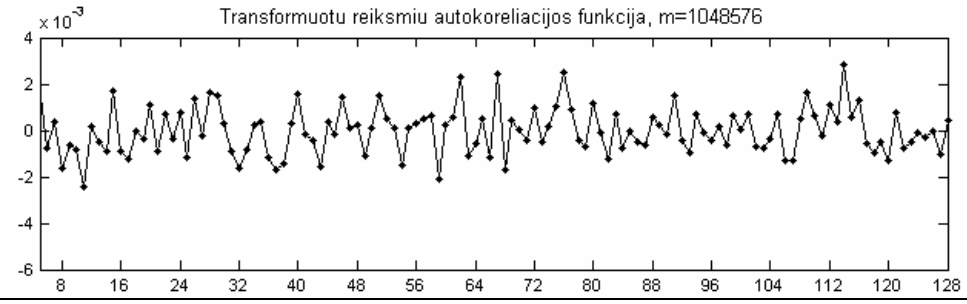
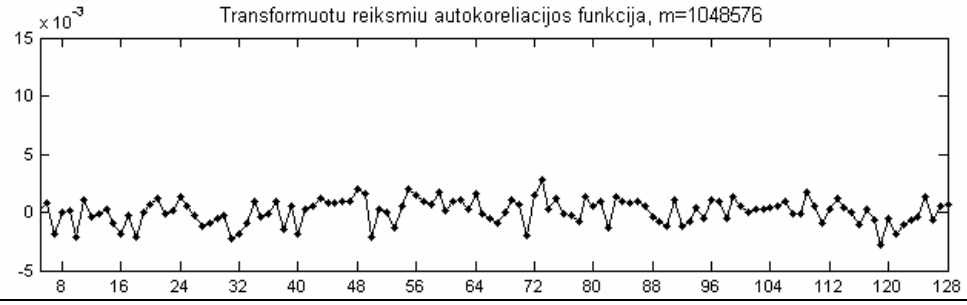
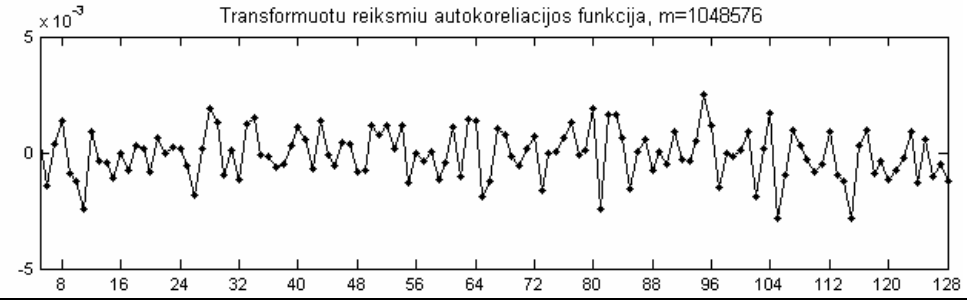
Transformacija tiese

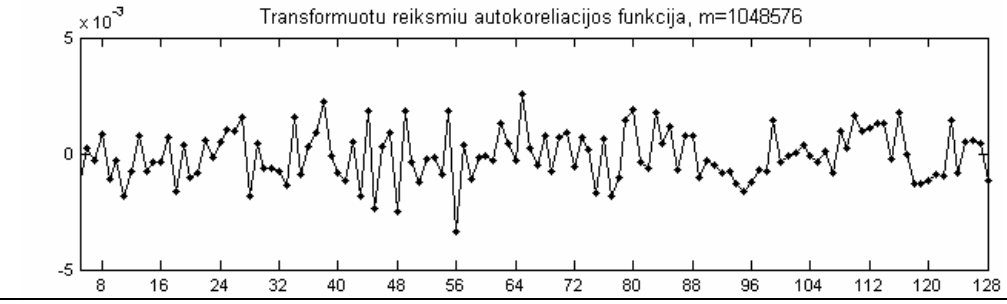
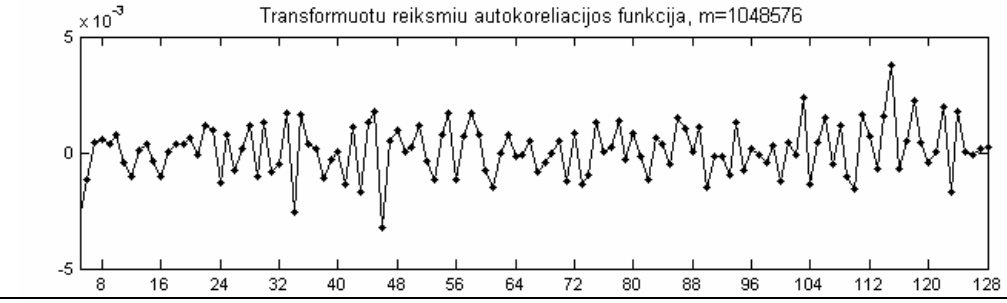
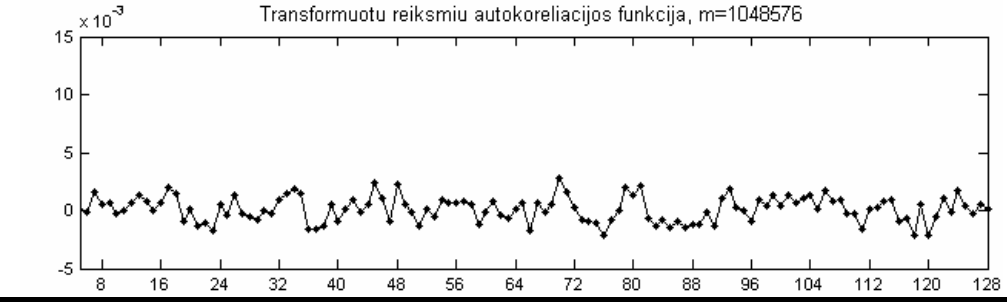
v1	$F(x)=\begin{cases}0, & \text{kai } x \le 0,\\ \dfrac{-\frac{0.00478}{2}x^2+0.03364x}{-\frac{0.00478}{2}+0.03364}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x \ge 1.\end{cases}$

v2	$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00563}{2}x^2+0.02844x}{\frac{0.00563}{2}+0.02844}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$$
v3	$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{-\frac{0.00684}{2}x^2+0.03467x}{-\frac{0.00684}{2}+0.03467}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$$
v4	$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00406}{2}x^2+0.02922x}{\frac{0.00406}{2}+0.02922}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$$
v5	$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{-\frac{0.00564}{2}x^2+0.03407x}{-\frac{0.00564}{2}+0.03407}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$$
v6	$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00474}{2}x^2+0.02888x}{\frac{0.00474}{2}+0.02888}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$$
v7	$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{-\frac{0.00411}{2}x^2+0.03330x}{-\frac{0.00411}{2}+0.03330}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$$
v8	$$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00683}{2}x^2+0.02783x}{\frac{0.00683}{2}+0.02783}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$$

6 lentelė

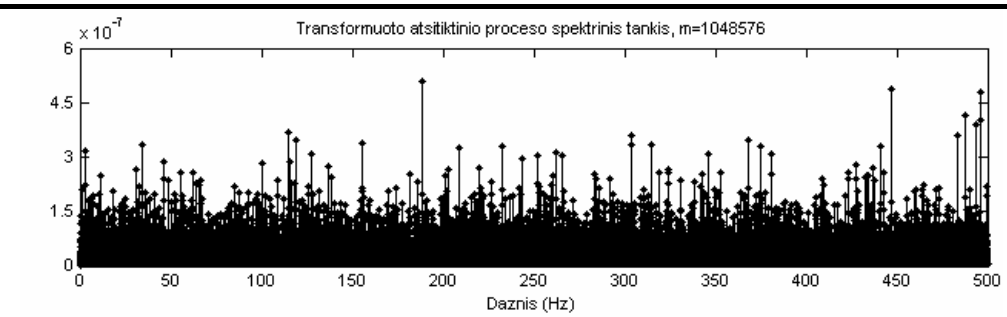
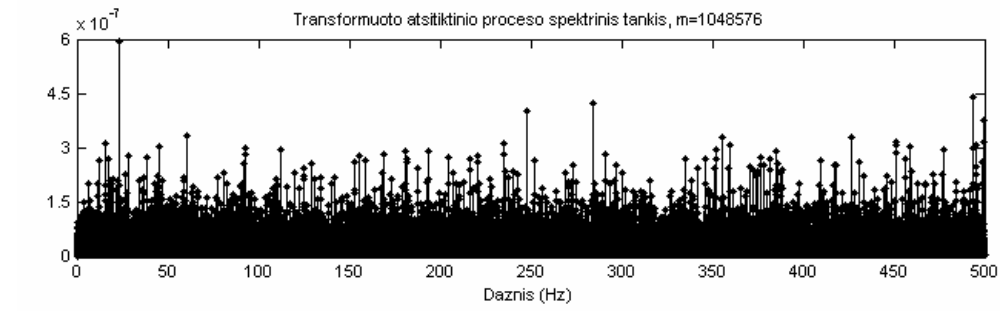
Transformuotų tiese atsitiktinių procesų autokoreliacijos funkcijos grafikai

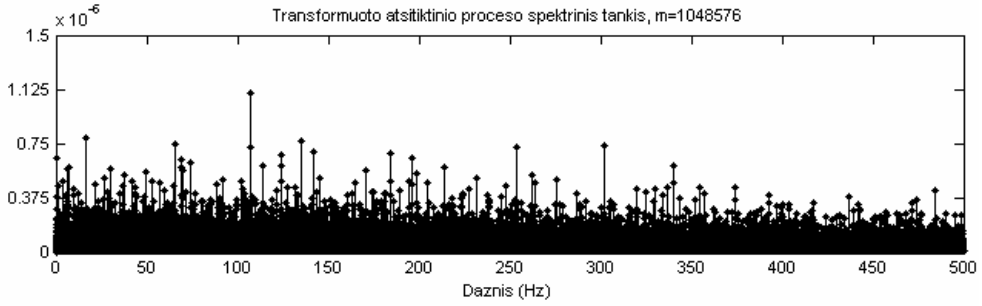
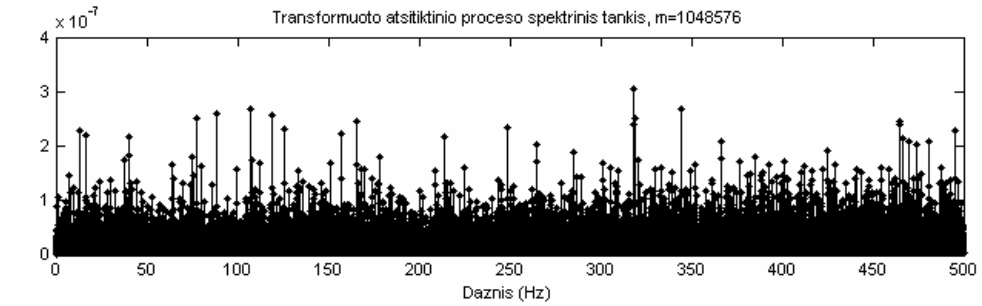
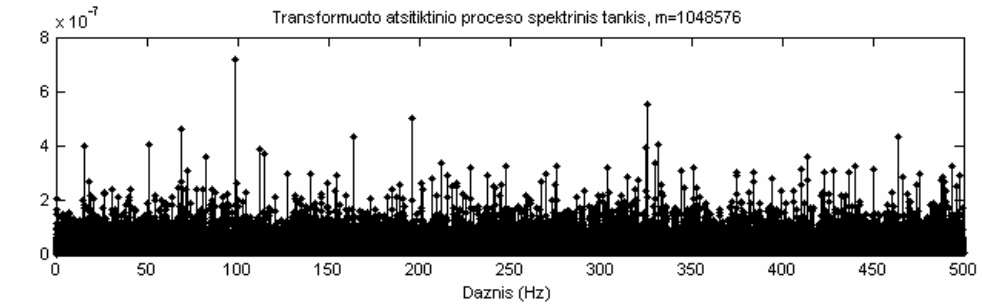
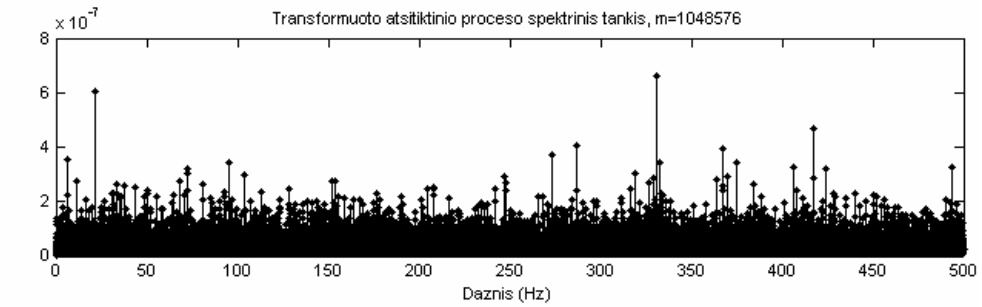
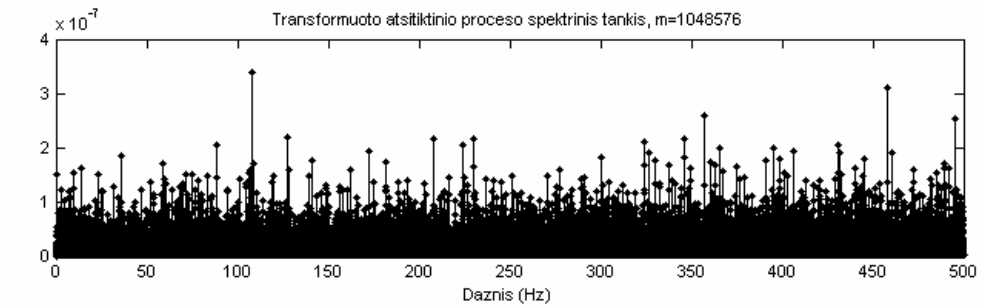
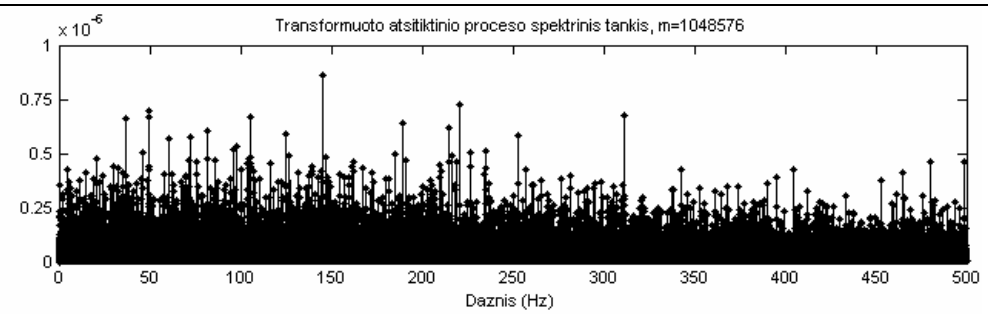
v1	
v2	
v3	
v4	
v5	

v6	
v7	
v8	

7 lentelė

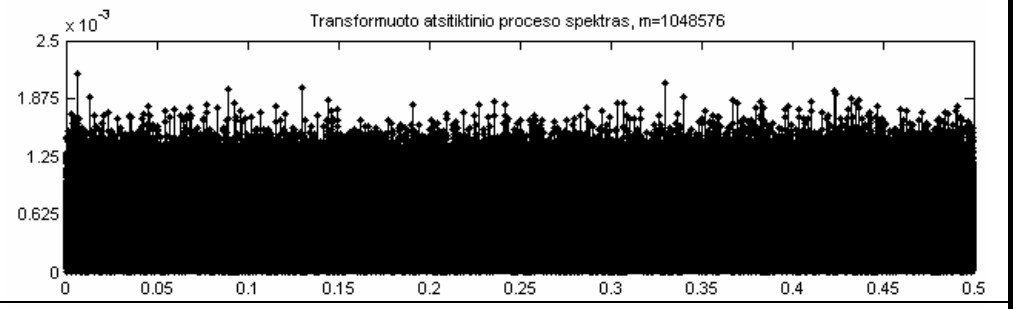
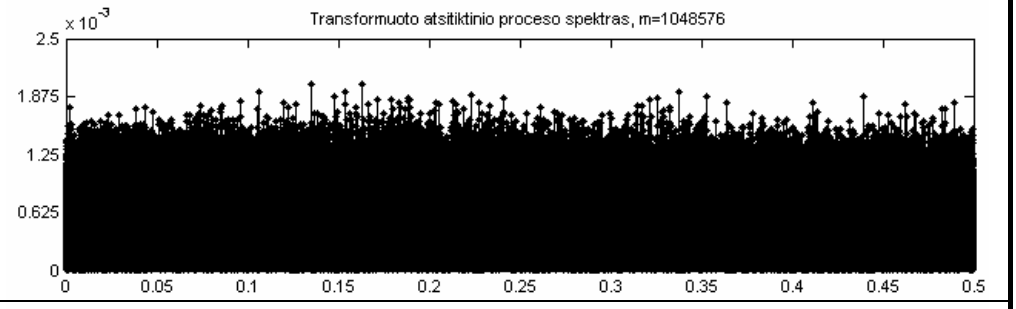
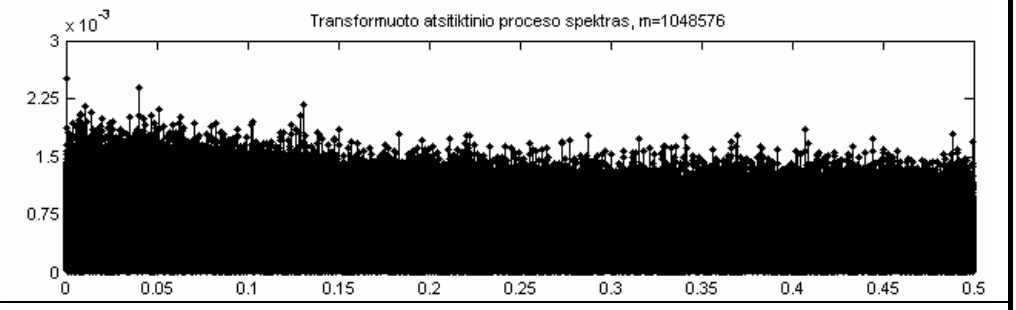
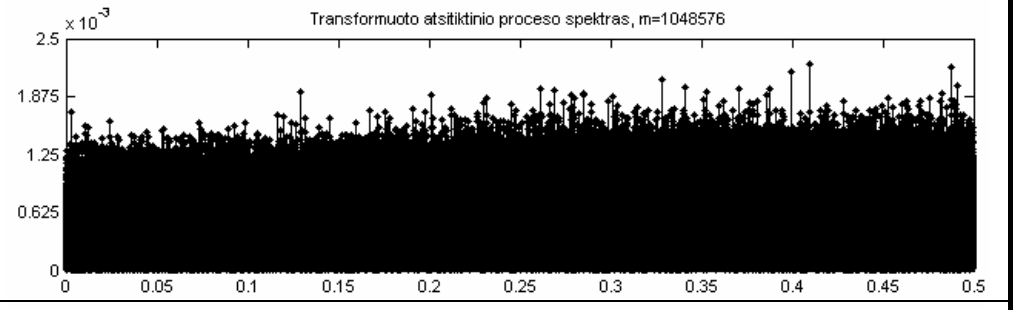
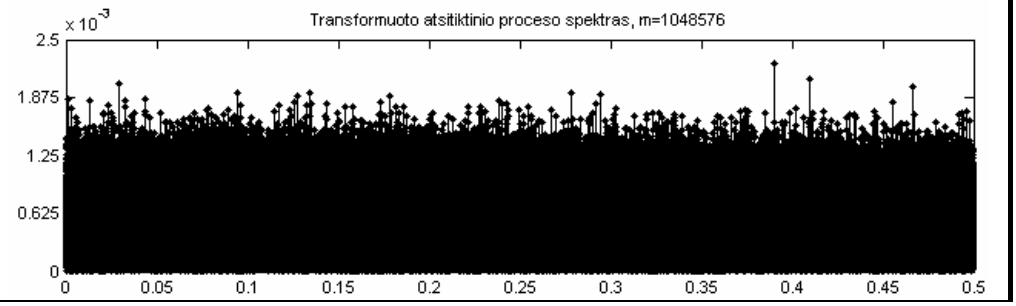
Transformuotų tiese atsitiktinių procesų spektrinio tankio grafikai

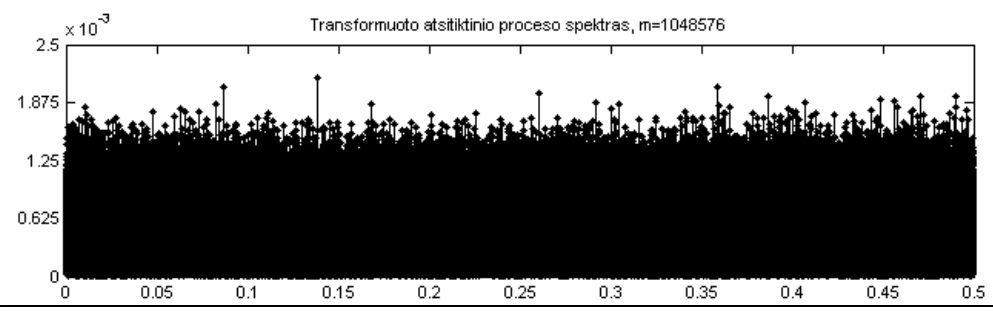
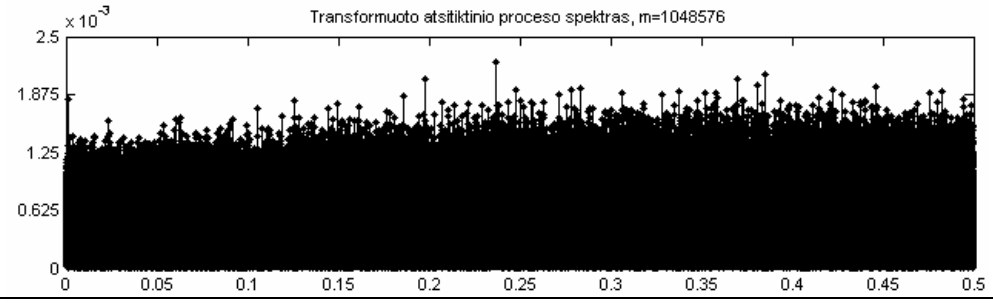
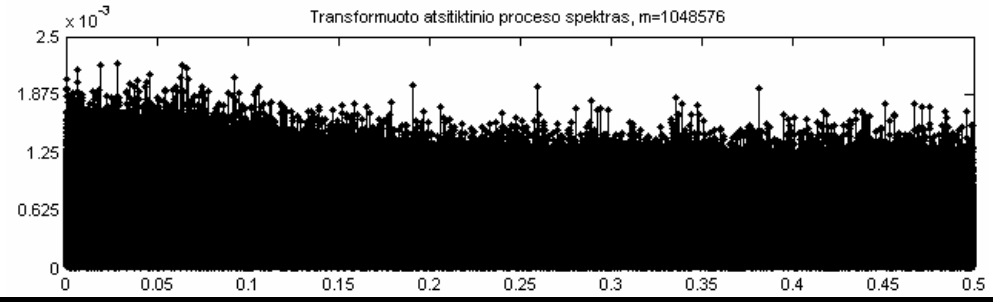
v1	
v2	

v3	
v4	
v5	
v6	
v7	
v8	

8 lentelė

Transformuotų tiese atsitiktinių procesų spektro grafikai

v1	
v2	
v3	
v4	
v5	

v6	
v7	
v8	

9 lentelė

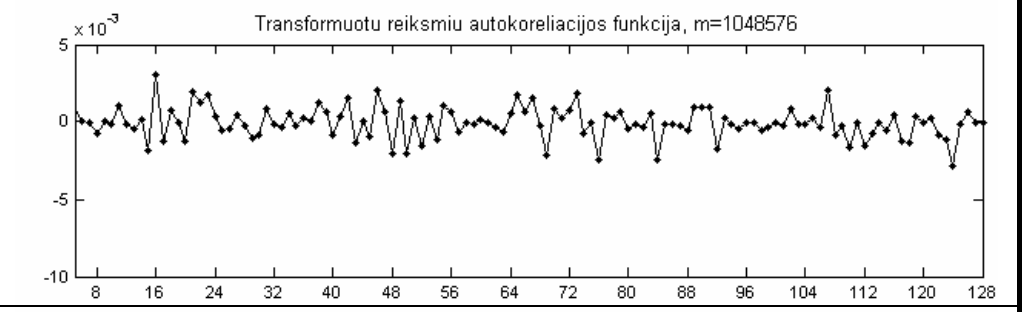
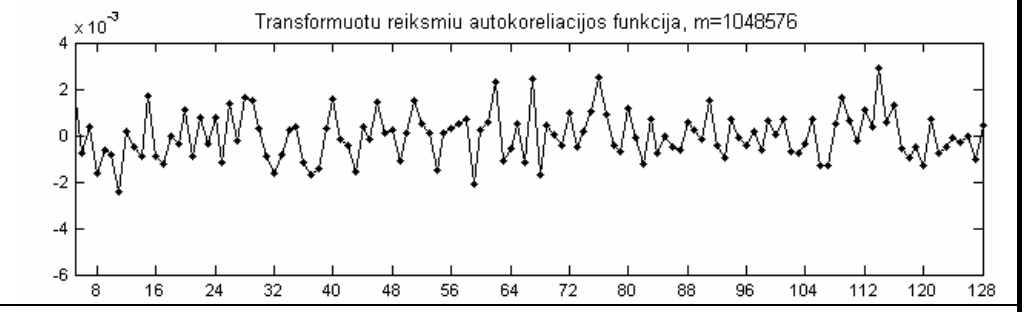
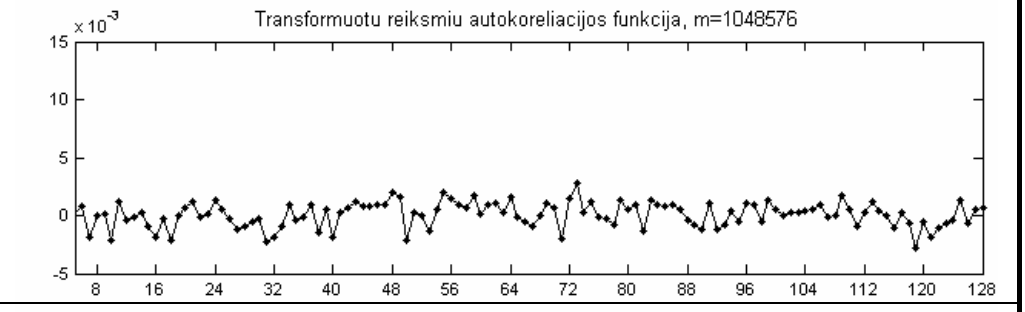
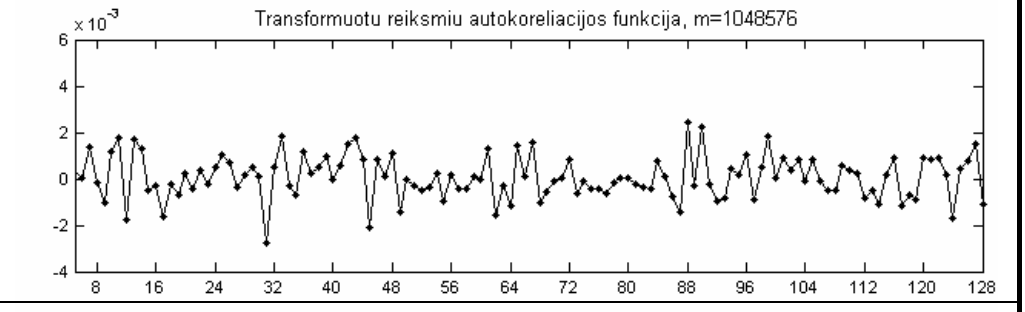
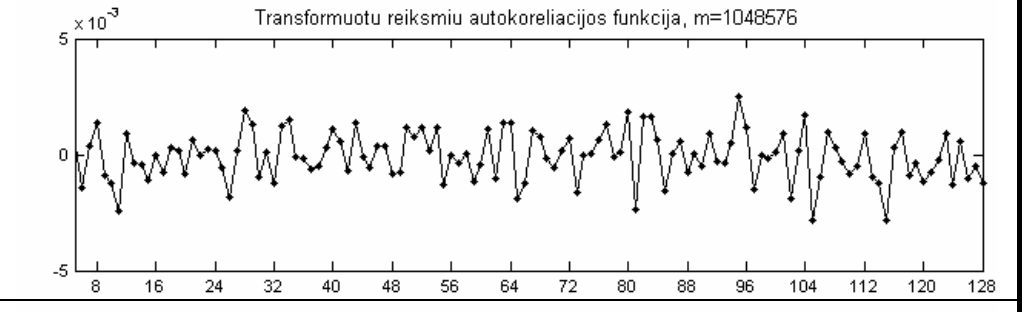
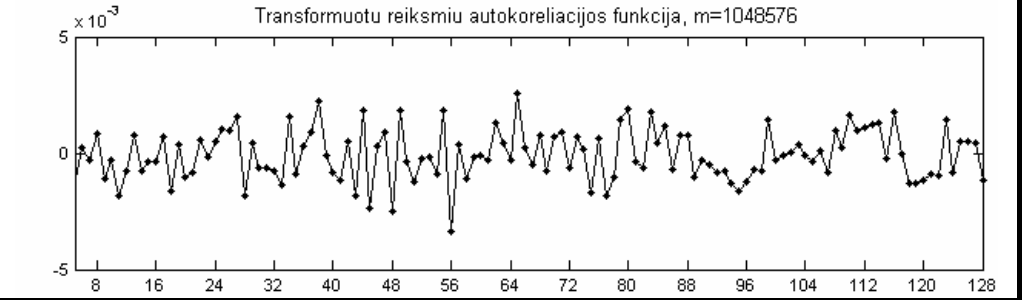
Transformacija parabole

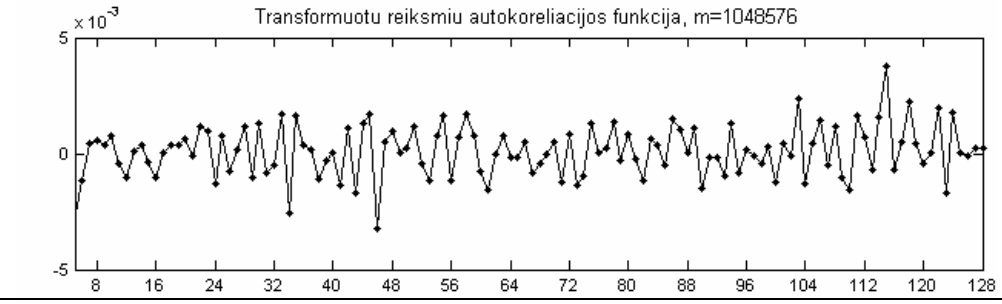
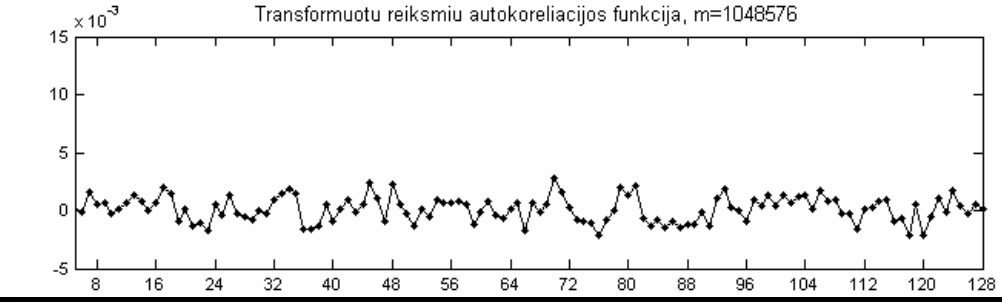
v1	$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00247}{3}x^3-\frac{0.00724}{2}x^2+0.03405x}{\frac{0.00247}{3}-\frac{0.00724}{2}+0.03405}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$
v2	$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00263}{3}x^3+\frac{0.00300}{2}x^2+0.02887x}{\frac{0.00263}{3}+\frac{0.00300}{2}+0.02887}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$

v3	$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00549}{3}x^3-\frac{0.01233}{2}x^2+0.03559x}{\frac{0.00549}{3}-\frac{0.01233}{2}+0.03559}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$
v4	$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00396}{3}x^3+\frac{0.00009943}{2}x^2+0.02988x}{\frac{0.00396}{3}+\frac{0.00009943}{2}+0.02988}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$
v5	$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00272}{3}x^3-\frac{0.00836}{2}x^2+0.03453x}{\frac{0.00272}{3}-\frac{0.00836}{2}+0.03453}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$
v6	$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00265}{3}x^3+\frac{0.00209}{2}x^2+0.02932x}{\frac{0.00265}{3}+\frac{0.00209}{2}+0.02932}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$
v7	$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00370}{3}x^3-\frac{0.00781}{2}x^2+0.03392x}{\frac{0.00370}{3}-\frac{0.00781}{2}+0.03392}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$
v8	$F(x)=\begin{cases}0, & \text{kai } x\le 0,\\ \dfrac{\frac{0.00545}{3}x^3+\frac{0.00138}{2}x^2+0.02874x}{\frac{0.00545}{3}+\frac{0.00138}{2}+0.02874}, & \text{kai } 0<x<1,\\ 1, & \text{kai } x\ge 1.\end{cases}$

10 lentelė

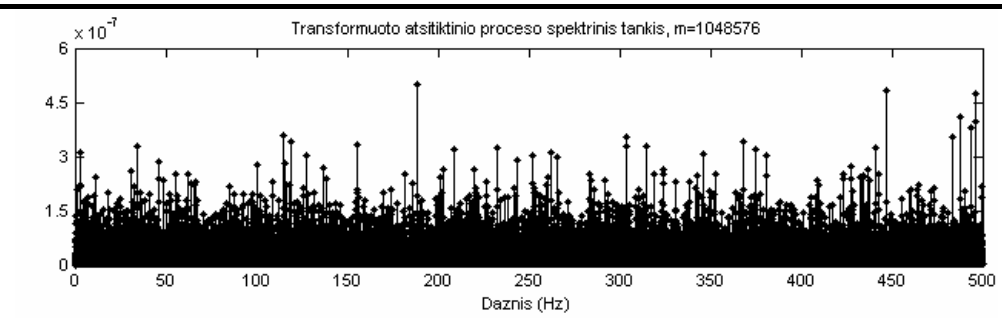
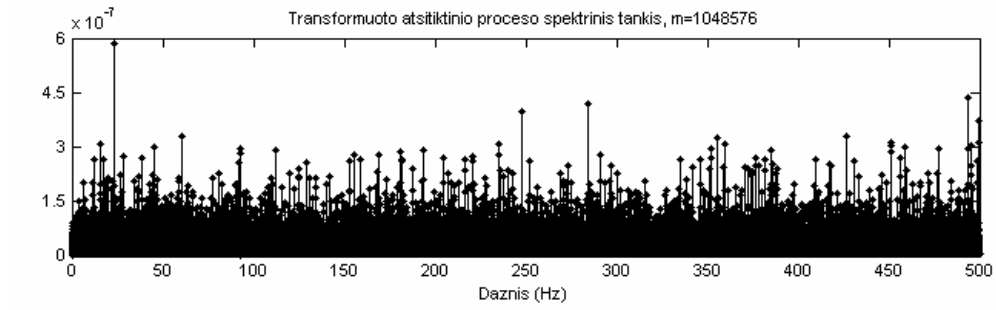
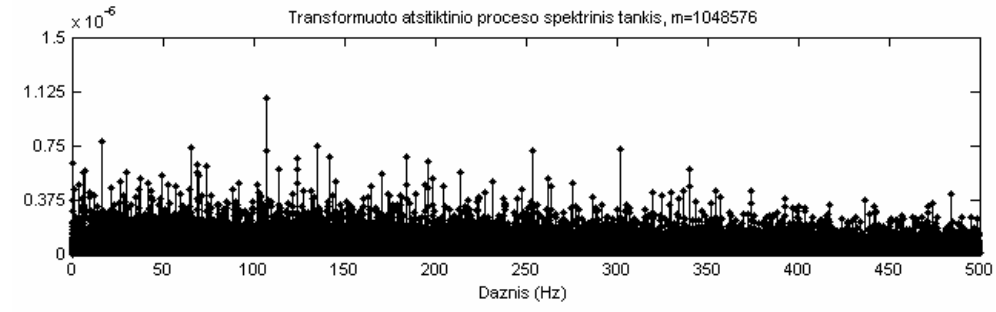
Transformuotų parabole atsitiktinių procesų autokoreliacijos funkcijos grafikai

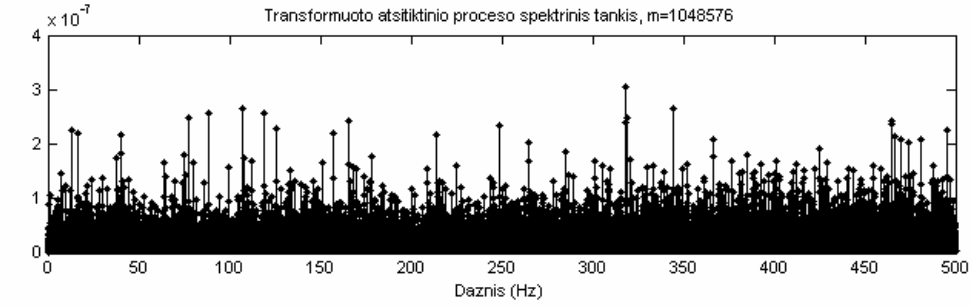
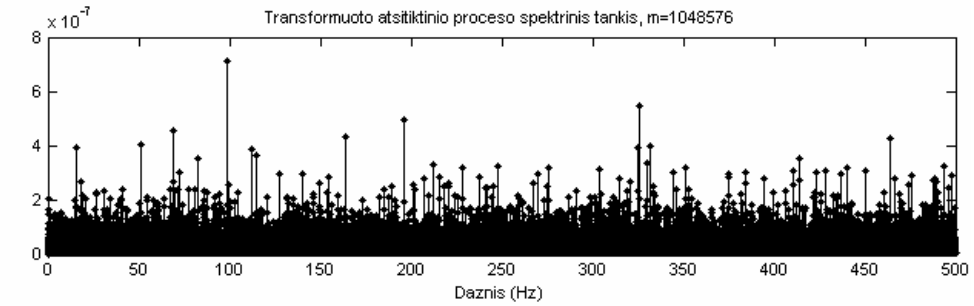
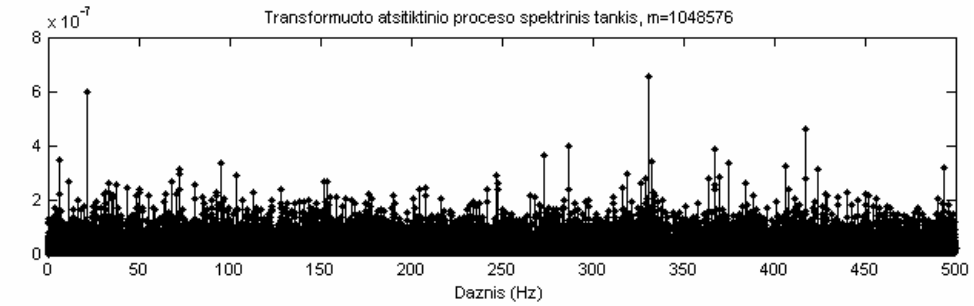
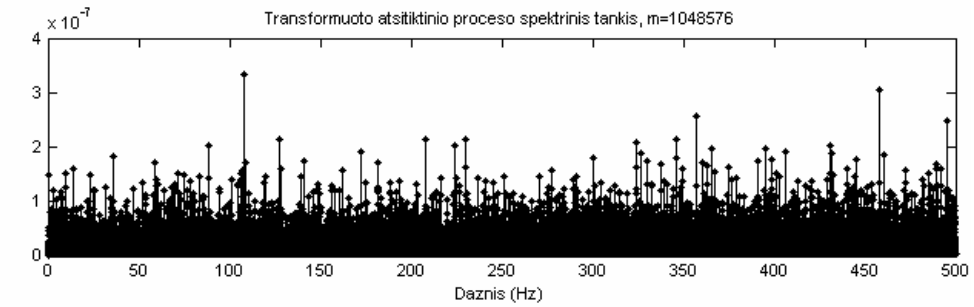
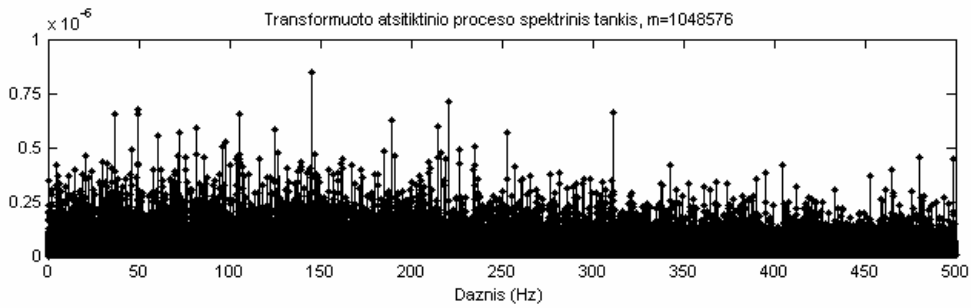
v1	
v2	
v3	
v4	
v5	
v6	

v7	
v8	

11 lentelė

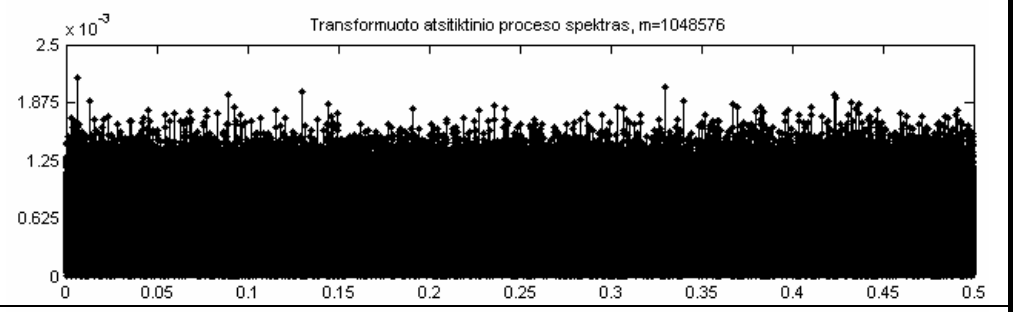
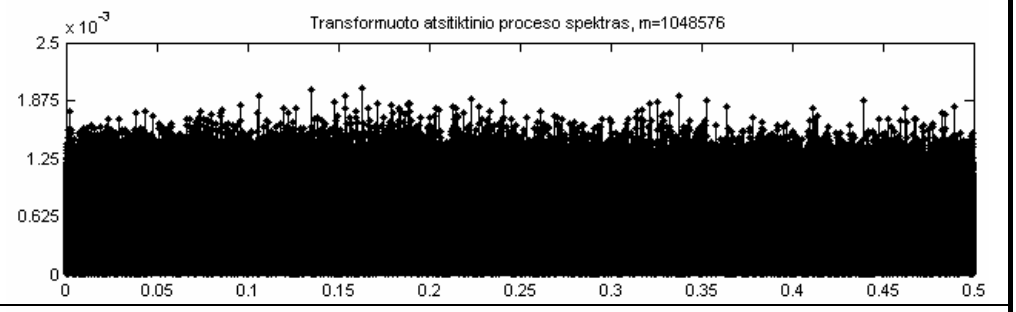
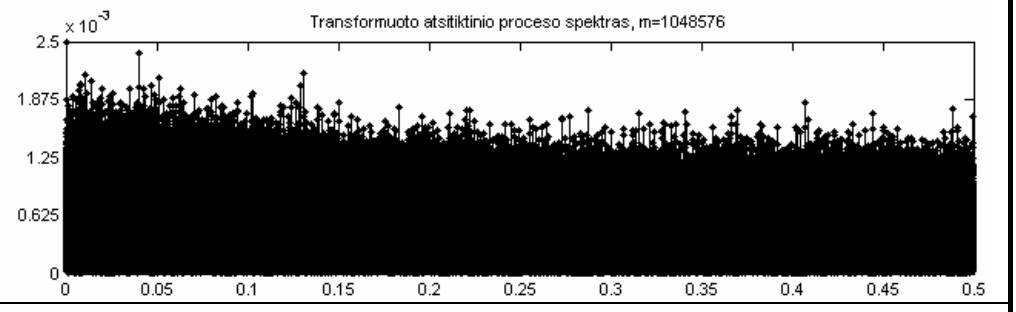
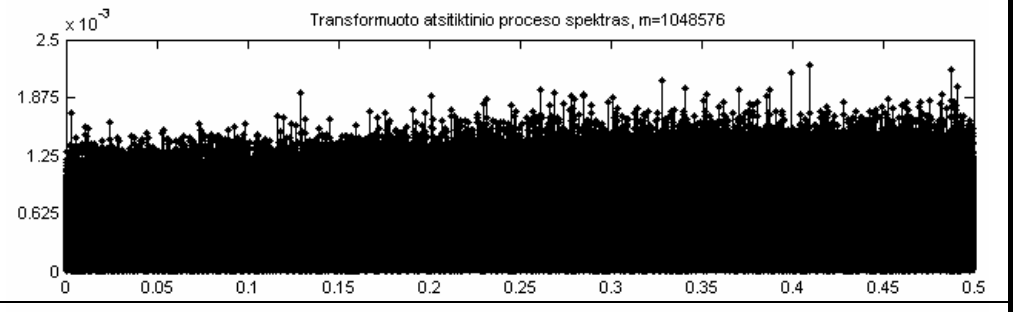
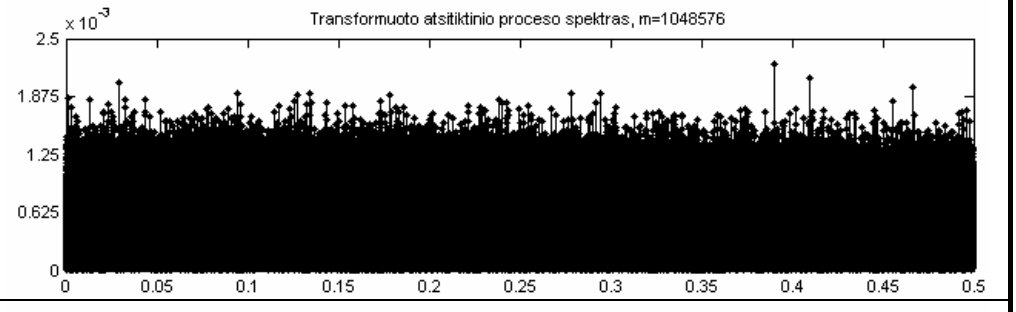
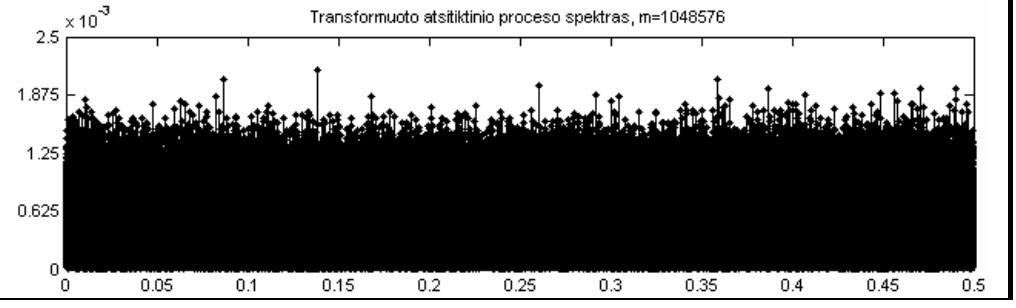
Transformuotų parabole atsitiktinių procesų spektrinio tankio grafikai

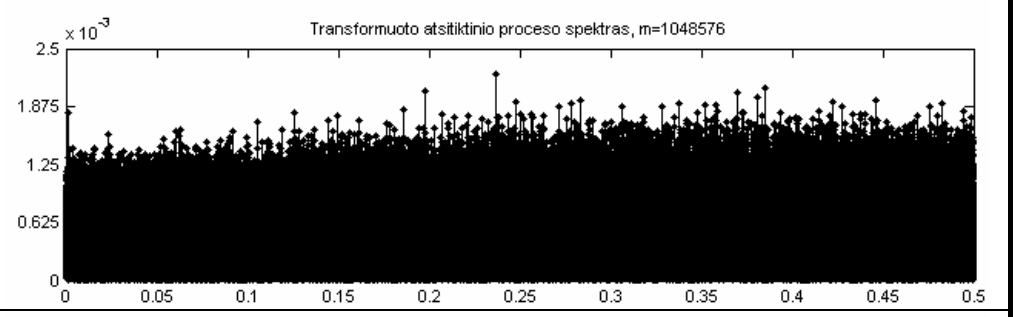
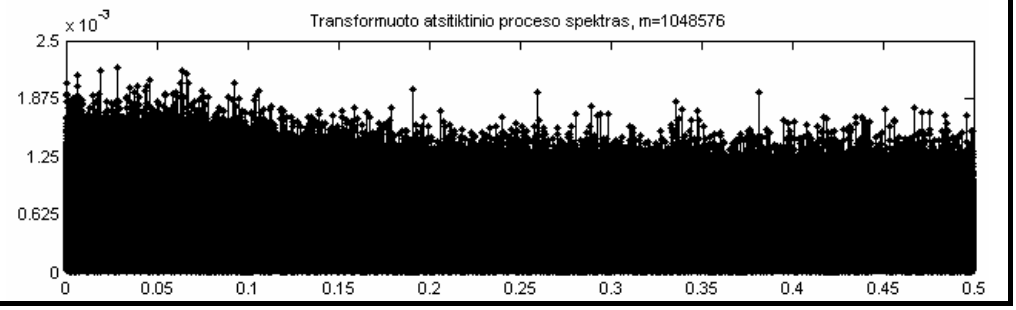
v1	
v2	
v3	

v4	
v5	
v6	
v7	
v8	

12 lentelė

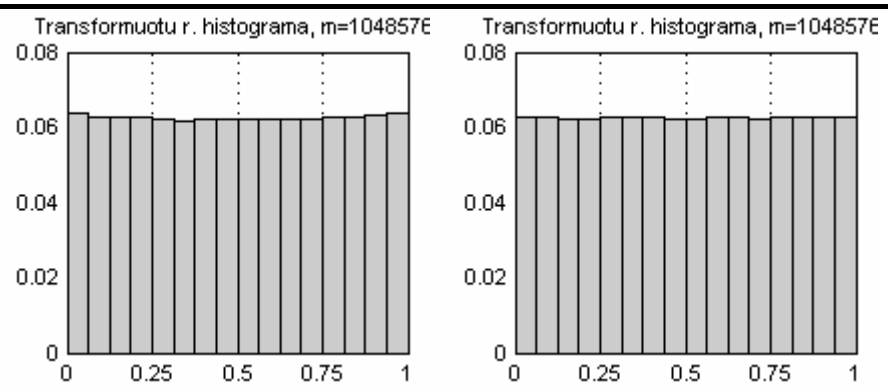
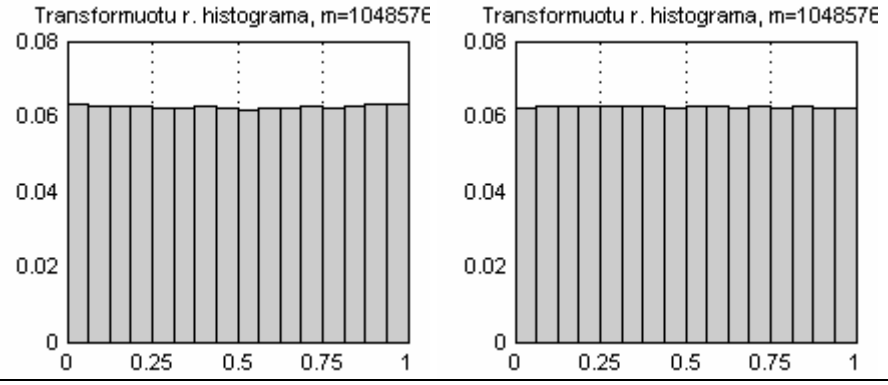
Transformuotų parabole atsitiktinių procesų spektro grafikai

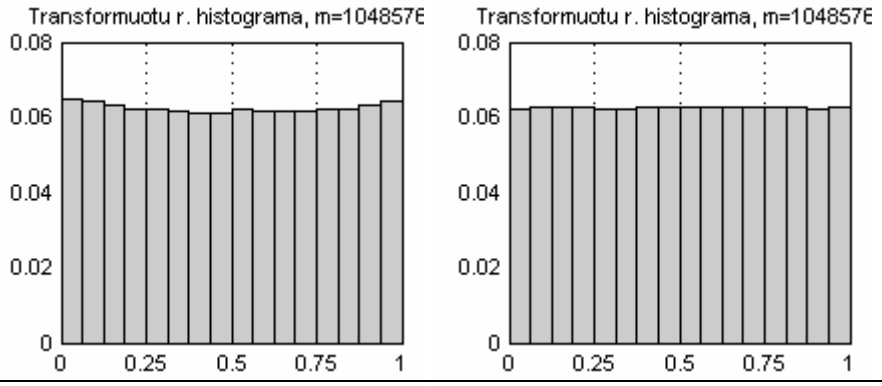
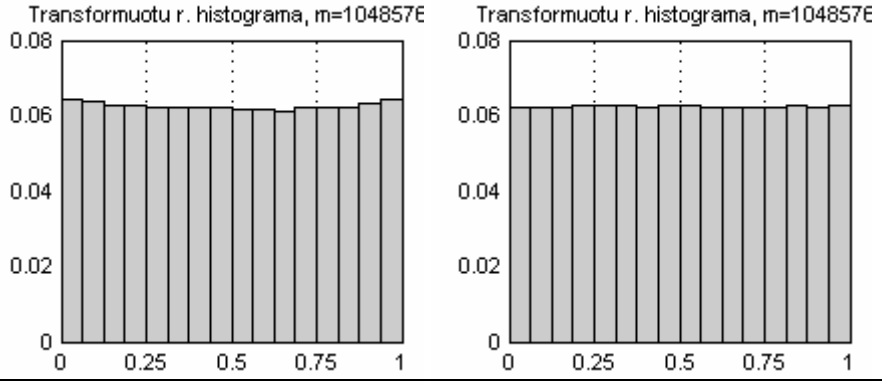
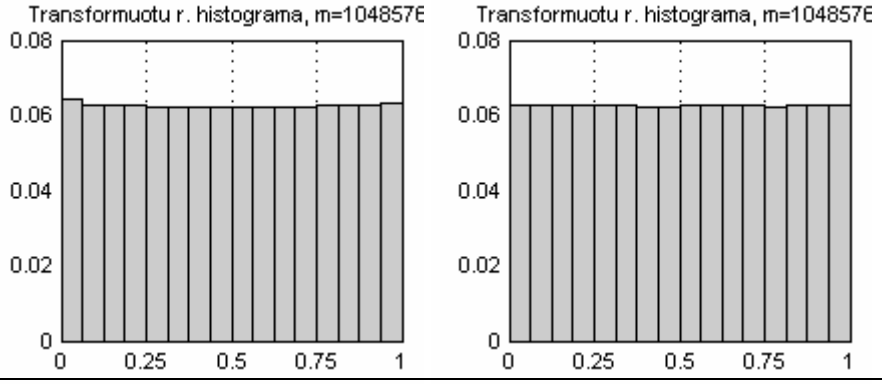
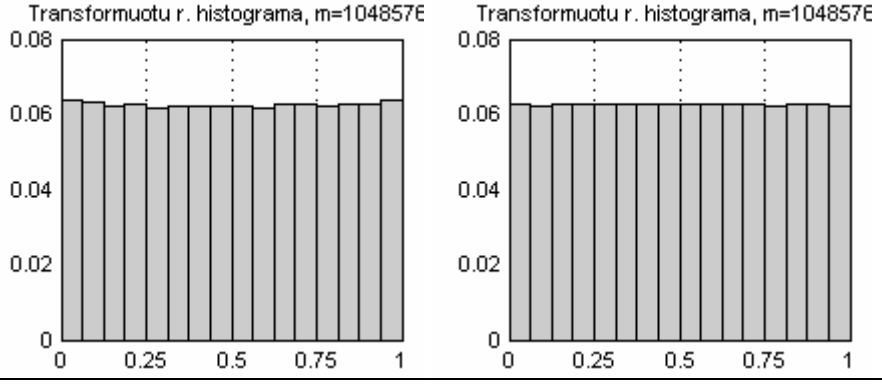
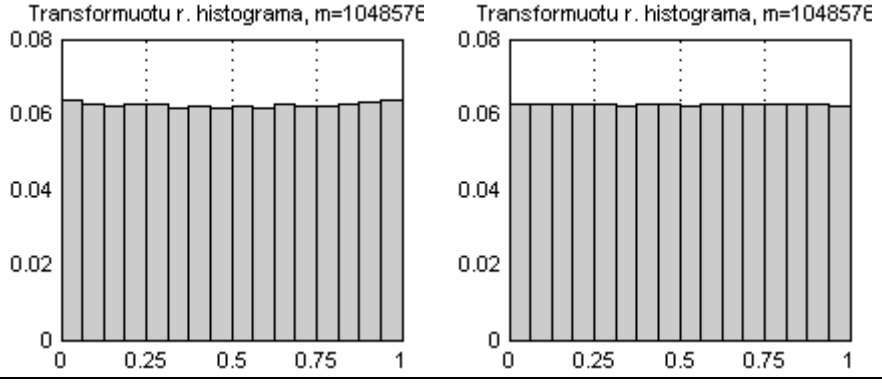
v1	
v2	
v3	
v4	
v5	
v6	

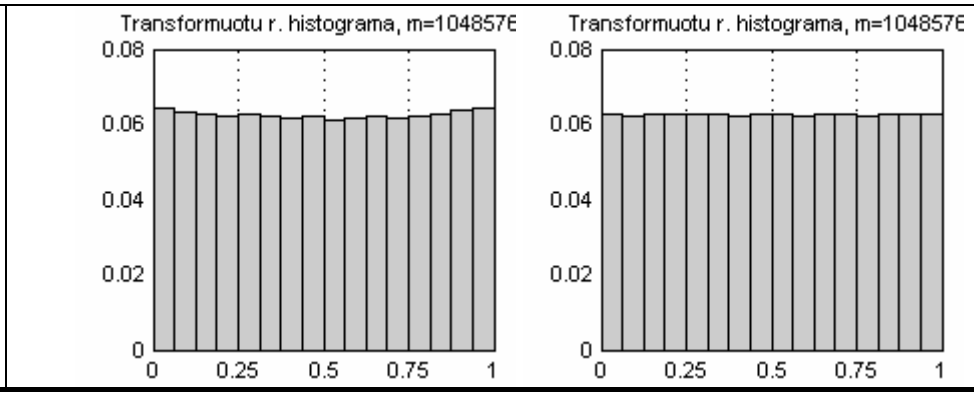
v7	
v8	

13 lentelė

Histogramos

v1	
v2	

v3	 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1
v4	 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1
v5	 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1
v6	 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1
v7	 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1

v8	 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1 Transformuotu r. histograma, m=104857E 0.08 0.06 0.04 0.02 0 0 0.25 0.5 0.75 1